EXHIBIT G

Trials@uspto.gov
Tel: 571-272-7822

Paper 37
Entered: September 24, 2020

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

APPLE INC.,
Petitioner,

v.

MPH TECHNOLOGIES OY,
Patent Owner.

IPR2019-00820
Patent 7,937,581 B2

Before KAMRAN JIVANI, JOHN D. HAMANN, and
STACY B. MARGOLIES, *Administrative Patent Judges.*

HAMANN, *Administrative Patent Judge.*

JUDGMENT
Final Written Decision
Determining Some Challenged Claims Unpatentable
35 U.S.C. § 318(a)

I. INTRODUCTION

In this *inter partes* review, instituted pursuant to 35 U.S.C. § 314, Apple Inc. ("Petitioner") challenges the patentability of claims 1–9 ("the challenged claims") of U.S. Patent No. 7,937,581 B2 (Ex. 1001, "the '581 patent"), owned by MPH Technologies Oy ("Patent Owner"). We have jurisdiction under 35 U.S.C § 6. This Final Written Decision is entered pursuant to 35 U.S.C. § 318(a) and 37 C.F.R. § 42.73.

For the reasons discussed herein, we determine that Petitioner has shown by a preponderance of the evidence that claims 1–3, 5, and 9 are unpatentable, but Petitioner has not shown by a preponderance of the evidence that claims 4 and 6–8 are unpatentable.

II. BACKGROUND

A. Procedural History

Petitioner filed a Petition requesting *inter partes* review of the challenged claims of the '581 patent. Paper 2 ("Pet."). The Petition is supported by the Declaration of David Goldschlag, Ph.D. (Ex. 1002). Patent Owner filed a Preliminary Response. Paper 8.

We instituted *inter partes* review of all of the challenged claims of the '581 patent on all of the grounds raised in the Petition. Paper 10 ("Dec. on Inst."), 7, 42. As to this Decision on Institution, Patent Owner filed a Request for Rehearing, and requested review by the Precedential Opinion Panel ("POP"). Paper 12; Ex. 3001. Patent Owner's request for POP review was denied, and we subsequently denied Patent Owner's Request for Rehearing. Papers 16, 24.

Patent Owner filed a replacement Response to the Petition. Paper 23 ("PO Resp."). The Response is supported by the Declaration of Professor

George N. Rouskas, Ph.D. (Ex. 2009). Petitioner filed a Reply to Patent Owner's Response. Paper 26 ("Pet. Reply"). The Reply is supported by an additional Declaration of David Goldschlag, Ph.D. (Ex. 1022). Patent Owner filed a Sur-Reply to Petitioner's Reply. Paper 29 ("PO Sur-Reply").

An oral hearing was held on June 25, 2020. A transcript of the oral hearing is included in the record. Paper 36 ("Tr.").

B. Related Matter

The parties identify *MPH Techs. Oy v. Apple Inc.*, No. 5:18-cv-05935-PJH (N.D. Cal.), as a matter that may affect or would be affected by a decision in this proceeding. Pet. 2–3; Paper 7, 1. The parties also identify, as a related matter, *Apple Inc. v. MPH Techs. Oy*, IPR2019-00819 (PTAB), involving U.S. Patent No. 7,620,810, which is the parent of the '581 patent. Pet. 2–3; Paper 7, 1.

C. The Challenged Patent (Ex. 1001)

The '581 patent relates to "secur[ing] mobile connections in telecommunication networks." Ex. 1001, 1:15–16. In particular, the '581 patent describes reducing the handover latency and computational overhead for secure connections, such as those employing Internet Protocol ("IP") Security ("IPSec") with mobile terminals[1] (i.e., terminals that can move from one network to another). *Id.* at 1:15–16, 1:59–66, 4:12–35, 6:42–44, 7:23–37, 10:31–39.

[1] The '581 patent discloses that "the term[s] mobility and mobile terminal do[] not only mean physical mobility, . . . [but also] mean[] moving from one network to another, which can be performed by a physically fixed terminal as well." Ex. 1001, 4:31–35.

IPSec comprises a set of rules defined by the Internet Engineering Task Force ("IETF") to "provide[] the capability to secure communications between arbitrary hosts," according to the '581 patent. *Id.* at 1:59–66, 2:5, 2:8–12. The '581 patent states that these rules describe, *inter alia*, providing "access control based on the distribution of cryptographic keys." *Id.* at 2:13–22. The '581 patent also describes the concept of a Security Association ("SA"), which according to the '581 patent is "a one-way relationship between a sender and a receiver that offers [negotiated] security services to the traffic carried on it." *Id.* at 2:24–26.

The '581 patent discloses that IPSec supports two modes of operation (i.e., transport mode and tunnel mode). *Id.* at 3:6–7. "Typically, transport mode is used for end-to-end communication between two hosts." *Id.* at 3:14–15. "Tunnel mode . . . is generally used for sending messages through more than two components," such as "when one or both ends of a SA is a security gateway, such as a firewall or a router that implements IPSec." *Id.* at 3:19–24.

"IPSec is intended to work with static network topolog[ies]," according to the '581 patent. *Id.* at 4:14–15. For example, IPSec can secure communications between hosts across a local area network ("LAN"), as well as across a private or public wide area network ("WAN"). *Id.* at 1:59–61. Figure 1, shown below, "illustrates an example of a telecommunication network to be used in the invention" of the '581 patent. *Id.* at 8:37–38.

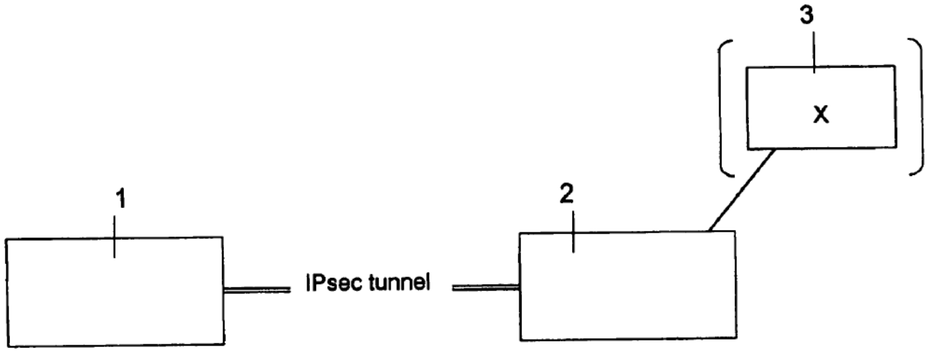


FIG. 1

Figure 1 depicts an example telecommunication network comprising "computer 1 . . . and computer 2[,] a destination computer, to which the secure messages are sent . . . by means of an IPSec tunnel established between computer 1 and computer 2." *Id.* at 8:50–55. The '581 patent adds: "Computer 2 [can] be a security gateway for a third computer 3. Then, the messages sent from computer 2 to computer 3 are sent in plaintext." *Id.* at 8:55–57.

The '581 patent discloses that in forming an IPSec tunnel under IPSec's default automated key management protocol (i.e., the Internet Key Exchange ("IKE") protocol), "the tunnel endpoints are fixed and remain constant." *Id.* at 4:2–7, 4:15–20. The '581 patent adds: "If IPSec is used with a mobile host, the IKE key exchange will have to be redone from every new[ly] visited network. This is problematic, because IKE key exchanges involve computationally expensive" calculations and require exchanging numerous messages between the endpoints, leading to higher latency. *Id.* at 4:18–29.

To address these problems, the '581 patent discloses avoiding a full re-negotiation between the tunnel endpoints, when computer 1 moves networks. *E.g.*, *id.* at 9:22–33 (describing prior art requires a full re-negotiation), 9:60–63. More specifically, the ’581 patent discloses initially establishing an IPSec tunnel between computer 1 (address A) and computer 2 (address X) using IKE, as in the prior art. *Id.* at 9:44–59, Fig. 5 (illustrating steps 1a–9a for setting up the tunnel); *compare id.* at Fig. 5, *with id.* at Fig. 4 (showing the same nine steps as the prior art solution); *see also id.* at 9:1–28 (describing the prior art IKE establishment of the tunnel).

The ’581 patent discloses that, when computer 1 moves from address A to address B, computer 1 sends from its new address (address B) to computer 2 (address X) at the other end of the established IPSec tunnel, a request for computer 2 to register its new address. *Id.* at 9:60–66. According to the ’581 patent, this request can be “encrypted and/or authenticated . . . us[ing] the same IPSec SA [that is used] for protecting both data and registration traffic.” *Id.* at 10:1–5.

The ’581 patent thus discloses that the tunnel’s IPSec SA is carried over to the new connection point, and computer 1 can send IPSec-protected messages to computer 2 after sending the request, which “essentially makes the handover latency zero.” *Id.* at 10:8–16, 10:31–34. “[T]he exact method of signalling is not important[;] the essence is to carry over the IPSec SA to the new connection point.” *Id.* at 10:8–10.

D. The Challenged Claims

Petitioner challenges claims 1–9 of the ’581 patent, of which claims 1 and 9 are independent. Claim 1 is illustrative of the challenged claims and is reproduced below:

> 1. A method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal

> and another terminal and a security gateway therebetween, the method comprising:
>
> a) establishing a secure connection having a first address of the mobile terminal as a first end-point and a gateway address of the security gateway as a second end-point,
>
> b) the mobile terminal changing from the first address to a second address,
>
> c) while at the second address, the mobile terminal sending a request message to the gateway address of the security gateway to request the security gateway to change the secure connection to be defined between the second address and the gateway address of the security gateway,
>
> in response to the request message from the mobile terminal, the security gateway changing an address definition of the secure connection from the first address to the second address, and
>
> the mobile terminal sending a secure message in the secure connection from the second address of the mobile terminal to the other terminal via the security gateway.

Ex. 1001, 10:50–11:3.

E. Instituted Grounds of Unpatentability

We instituted trial based on the following grounds of unpatentability, which are all the grounds of unpatentability raised in the Petition:

	References	**Basis**[2]	**Challenged Claim(s)**
1.	Ishiyama,[3] Murakawa[4]	§ 103(a)	1, 2, 4, 6, 7, 9
2.	Ishiyama, Murakawa, Ahonen[5]	§ 103(a)	3, 5

[2] The Leahy-Smith America Invents Act ("AIA") included revisions to 35 U.S.C. § 103 that became effective on March 16, 2013. Because the '581 patent issued from an application filed before March 16, 2013, we apply the pre-AIA version of the statutory basis for unpatentability.
[3] U.S. Patent No. 6,904,466 B1 (issued June 7, 2005) (Ex. 1004).
[4] U.S. Patent No. 7,028,337 B2 (issued Apr. 11, 2006) (Ex. 1005).
[5] U.S. Patent No. 6,976,177 B2 (issued Dec. 13, 2005) (Ex. 1006).

3.	Ishiyama, Murakawa, Forslöw[6]	§ 103(a)	8

Pet. 4, 11–64.

III. LEVEL OF ORDINARY SKILL IN THE ART

To determine whether an invention would have been obvious at the time it was made, we consider the level of ordinary skill in the pertinent art at the time of the invention. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). In assessing the level of ordinary skill in the art, various factors may be considered, including the "type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field." *In re GPAC, Inc.*, 57 F.3d 1573, 1579 (Fed. Cir. 1995) (citing *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962 (Fed. Cir. 1986)). "[O]ne or more factors may predominate." *Id.*

In our Decision on Institution, we adopted Petitioner's proposed definition for one having ordinary skill in the art at the time of the invention of the '581 patent as one who "would have had a B.S. degree in Computer Engineering, Electrical Engineering, or an equivalent field, as well as at least 3–5 years of academic or industry experience in the Internet security industry." Pet. 11 (citing Ex. 1002 ¶¶ 20–21). Patent Owner does not dispute our adoption of Petitioner's definition, nor otherwise address the level of ordinary skill at the time of the invention of the '581 patent. *See generally* PO. Resp.

Because Petitioner's definition of the level of skill in the art is consistent with the '581 patent and the asserted prior art, we maintain

[6] U.S. Patent No. 6,954,790 B2 (issued Oct. 11, 2005) (Ex. 1007).

Petitioner's definition for purposes of this Final Written Decision. *See Okajima v. Bourdeau*, 261 F.3d 1350, 1355 (Fed. Cir. 2001); *GPAC*, 57 F.3d at 1579; *In re Oelrich*, 579 F.2d 86, 91 (CCPA 1978). We apply Petitioner's definition in our analysis below.

IV. CLAIM CONSTRUCTION

Because the Petition was filed after November 13, 2018, we construe the challenged claims by applying "the standard used in federal courts, in other words, the claim construction standard that would be used to construe the claim in a civil action under 35 U.S.C. [§] 282(b), which is articulated in *Phillips* [*v. AWH Corp.*, 415 F.3d 1303 (Fed. Cir. 2005) (en banc)]." *See* Changes to the Claim Construction Standard for Interpreting Claims in Trial Proceedings Before the Patent Trial and Appeal Board, 83 Fed. Reg. 51,340, 51,340, 51,358, 51,343–44 (Oct. 11, 2018) (amending 37 C.F.R. § 42.100(b) effective November 13, 2018) (now codified at 37 C.F.R. § 42.100(b) (2019)). Under *Phillips*, the words of a claim are generally given their "ordinary and customary meaning," which is the meaning they would have to a person of ordinary skill in the art at the time of the invention, in light of the specification and prosecution history. *See Phillips*, 415 F.3d at 1312–13.

Petitioner does not submit any terms for construction. Pet. 11 (arguing that "[a]ll claim terms of the '581 patent should receive their ordinary and customary meaning"). Patent Owner submits the term "security gateway" for construction, and argues that its meaning is in dispute. PO Resp. 10–24. To show a dispute, Patent Owner quotes from our Decision on Institution where we preliminarily found that (i) "Petitioner argues that one of ordinary skill in the art would have understood that Ishiyama's 'correspondent [host]' would be a security gateway," and

(ii) "there [wa]s sufficient support in the [preliminary] record that Ishiyama's correspondent host is a security gateway." PO Resp. 10–11 (citing Dec. on Inst. 26, 34). Patent Owner argues "[t]hus, the claim construction dispute in this proceeding is whether a correspondent host is a 'security gateway.'" *Id.* at 11.

For our analysis below, however, we do not rely on Petitioner's arguments that Ishiyama's correspondent host is a security gateway. Rather, we consider Petitioner's alternative argument[7] that Murakawa teaches a security gateway. Thus, we conclude that no express claim construction is necessary to determine whether Petitioner has shown by a preponderance of evidence that the challenged claims are unpatentable. *See, e.g.*, *Nidec Motor Corp. v. Zhongshan Broad Ocean Motor Co.*, 868 F.3d 1013, 1017 (Fed. Cir. 2017) (quoting *Vivid Techs., Inc. v. Am. Sci. & Eng'g, Inc.*, 200 F.3d 795, 803 (Fed. Cir. 1999)) ("[W]e need only construe terms 'that are in controversy, and only to the extent necessary to resolve the controversy.'").

V. PRINCIPLES OF LAW

A claim is unpatentable under 35 U.S.C. § 103(a) if the differences between the claimed subject matter and the prior art are such that the subject matter, as a whole, would have been obvious at the time of the invention to a person having ordinary skill in the art. *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 406 (2007). The question of obviousness is resolved on the basis of underlying factual determinations, including (1) the scope and content of

[7] "Petitioner alternatively relies on Ishiyama's teachings combined with Murakawa's teachings of a 'security gateway configuration' (e.g., 'a security gateway' and 'another terminal'/'other terminal'") for disclosing claim 1." Dec. on Inst. 25; *see also* Pet. 11–53.

the prior art; (2) any differences between the claimed subject matter and the prior art; (3) the level of ordinary skill in the art; and (4) objective evidence of non-obviousness, if present.[8] *See Graham*, 383 U.S. at 17–18. When evaluating a claim for obviousness, we also must "determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *KSR*, 550 U.S. at 418 (citing *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006)).

VI. ALLEGED OBVIOUSNESS OVER ISHIYAMA AND MURAKAWA

Petitioner argues that the combination of Ishiyama and Murakawa renders claims 1, 2, 4, 6, 7, and 9 of the '581 patent obvious under 35 U.S.C. § 103(a). Pet. 11–53. We have reviewed the parties' arguments and the evidence of record. For the reasons that follow, we determine that Petitioner (1) shows by a preponderance of the evidence that claims 1, 2, and 9 would have been obvious to one of ordinary skill in the art in view of Ishiyama and Murakawa; and (2) fails to show by a preponderance of the evidence that claims 4, 6, and 7 would have been obvious to one of ordinary skill in the art in view of Ishiyama and Murakawa.

A. Summary of Ishiyama

Ishiyama relates to improving a mobile computer's "capab[ility] of carrying out communications while moving among a plurality of inter-connected networks." Ex. 1004, 1:9–11. In furtherance of this mobility, Ishiyama discloses having the mobile computer notify its correspondent host (i.e., the host at the other end of a communication) of its new address when

[8] Patent Owner does not present arguments or evidence of such objective evidence of non-obviousness in its Response. *See generally* PO Resp.

the mobile computer moves networks. *E.g.*, *id.* at 3:43–67, 6:13–18, 15:37–16:10. The mobile computer makes this notification by changing the source address of an outer packet of an encapsulated packet to the mobile computer's new address before sending the packet to the correspondent host. *Id.* When the correspondent host receives the packet from the mobile computer, the correspondent host detects the address change and updates its stored information to reflect the new address for the mobile computer. *E.g.*, *id.* at 3:9–14.

Figure 4, shown below, is a schematic diagram illustrating a mobile computer changing locations in an exemplary configuration of a mobile communication system, in accordance with an embodiment of Ishiyama's invention. *Id.* at 5:5–7, 5:11–13.

FIG. 4

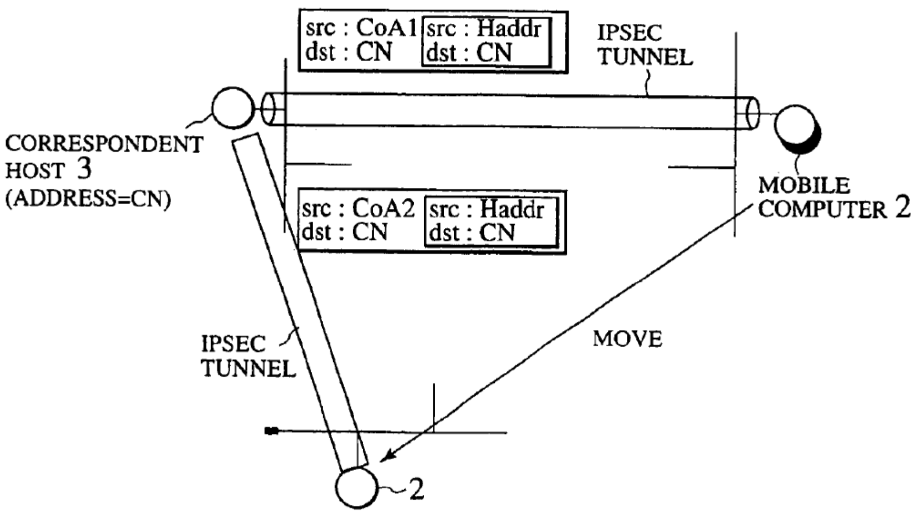


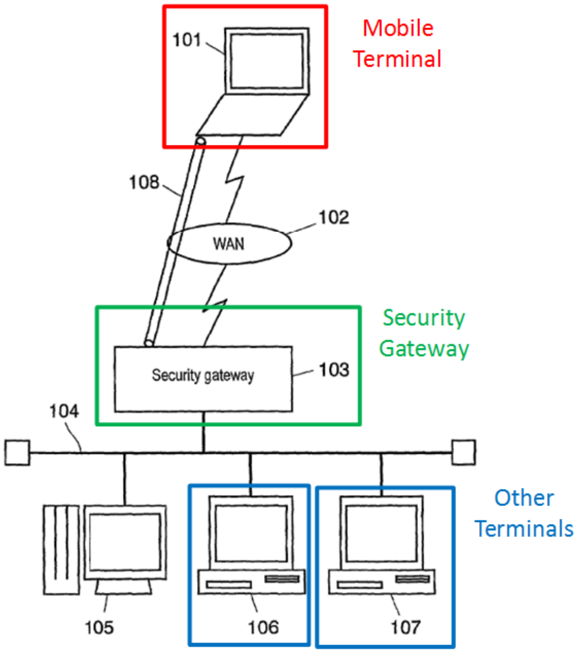
Figure 4 "shows an exemplary situation in which a packet is transferred from mobile computer 2 to . . . correspondent host 3 using [an] IPSEC tunnel." *Id.* at 8:33–35. Initially, mobile computer 2 communicates with correspondent host 3 via an IPSec tunnel, with mobile computer 2's address (CoA1) indicating its endpoint of the tunnel. *Id.* at 8:43–49. In other words, "mobile computer 2 transmits an encapsulated packet in which the outer packet has the source address='CoA1' and the destination address='CN.'" *Id.* at 8:50–54. As shown, when mobile computer 2 moves, its address changes from CoA1 to CoA2. *Id.* at 8:55–58, Fig. 4 (showing that mobile computer 2 moves networks). To convey this change, mobile computer 2 changes the source address of the outer packet to CoA2 and transmits the packet to correspondent host 3 via the IPSec tunnel. *Id.* at 8:59–63, Fig. 4. Correspondent host 3 detects this change in mobile computer 2's address, and replaces the CoA1 address with CoA2 in its database for the IPSec tunnel. *Id.* at 8:66–9:4; *see also id.* at Figs. 9B, 9D (showing the update of the address in correspondent host 3's SA database), 12:51–59. Ishiyama discloses that the other SA information "remain[s] unchanged, so that there is no need to re-negotiate keys for IPS[ec] encryption and authentication." *Id.* at 9:5–10.

B. Summary of Murakawa

Murakawa relates to allowing a PC outside a LAN to be virtually regarded as a PC on the LAN and communicate with a terminal on the LAN. Ex. 1005, 1:16–24, 3:62–65. Specifically, Murakawa discloses allowing an outside terminal to communicate (via a WAN, a security gateway, and a LAN) with a terminal on the LAN. *Id.* at 1:11–24, 3:61–4:16.

Petitioner's annotated version of Murakawa's Figure 5, which illustrates a "prior art typical network system," *id.* at 4:32–33, is shown below.

FIG. 5 PRIOR ART



Murakawa's Figure 5 above shows a "prior art typical network system" and is further annotated by Petitioner to add labels for a mobile terminal, security gateway, and other terminals. Pet. 28. According to Murakawa, Figure 5 "is a block diagram of a typical network system including a WAN." Ex. 1005, 1:51–53. As shown in Figure 5, the network system includes "PC 101 [(labeled by Petitioner as 'Mobile Terminal')], which is located outside . . . LAN [104 and] establish[es] a dialup connection to the provider, WAN 102, and security gateway 103 [(labeled by Petitioner as 'Security Gateway')] that connects WAN 102 and LAN 104." *Id.* at 1:54–58. In addition, "LAN 104[,] being subjected to security gateway 103[,] includes . . . client PCs 106, 107" (labeled by Petitioner as "Other Terminals"). *Id.* at 1:59–60. Also shown is virtual private network ("VPN") 108, which is established between PC 101 and security gateway 103 to perform IPSec communication. *Id.* at 1:61–63. Murakawa discloses that this network system ensures safe communications between PC 101 and the terminals on LAN 104. *Id.* at 2:1–4.

C. Challenged Claim 1

Claim 1 is an independent claim. Petitioner combines Ishiyama and Murakawa in two alternative ways in arguing that claim 1 would have been obvious to one of ordinary skill in the art. *See* Pet. 11–47; Dec. on Inst. 25, 38–39 (noting the two alternative ways). Below we address Petitioner's second way of combining Ishiyama and Murakawa (i.e., combining Ishiyama's address changing functionality with Murakawa's security gateway and another terminal)). In other words, Petitioner combines Ishiyama's "address updating for a mobile terminal operating in the IPSec tunneling mode" with "Murakawa's . . . security gateway configuration" for "tunneling of communications through a security gateway so that two terminals are able to communicate." *E.g.*, Pet. 20 (citing Ex. 1004, 7:46–49; Ex. 1005, 4:13–16; Ex. 1002 ¶ 61). For that combination, we find that Petitioner demonstrates by a preponderance of the evidence that claim 1 would have been obvious to one of ordinary skill in the art. Because of this finding, we do not reach the parties' arguments concerning the first way Petitioner combines Ishiyama and Murakawa. For example, we do not reach whether Ishiyama teaches that its correspondent host is a security gateway.

1. Preamble

Claim 1's preamble recites "[a] method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal and a security gateway therebetween." Ex. 1001, 10:50–53. We agree with Petitioner and find that the combination of Ishiyama and Murakawa teaches claim 1's preamble.

Pet. 20–26. As we find that Ishiyama and Murakawa teach the preamble, we need not determine whether the preamble is limiting.

As to Ishiyama, we agree with Petitioner that Ishiyama teaches "a mobile communication scheme capable of easily changing a connected location of a mobile computer on [an] IP network." Ex. 1004, 2:42–45; Pet. 21. More specifically, we find that Ishiyama teaches using care-of addresses ("CoA") for a "mobile computer 2 [that] always uses the IPSEC in the tunnel mode at a time of making a connection to the correspondent host 3." Ex. 1004, 7:66–67, 11:9–16; Pet. 21.

As to Murakawa, we agree with Petitioner and find that Murakawa teaches forwarding messages received from a terminal at a security gateway located between the terminal and another terminal. *E.g.*, Ex. 1005, Fig. 5; Pet. 24 (annotating Ex. 1005, Fig. 5). As illustrated in Figure 5, Murakawa discloses that PC 101 establishes an IPSec tunnel (VPN 108), with security gateway 103. Ex. 1005, 1:61–63, 2:62–65, Fig. 5; Pet. 24–25. Murakawa's security gateway 103 connects to PC 106 and PC 107. Ex. 1005, 1:59–60. We agree with Petitioner and find that either PC 106 or PC 107 is the claimed another terminal. *Id.* at 1:61–2:4, Fig. 5; *see also* Pet. 24–25 (annotating Ex. 1005, Fig. 5 (labeling PC 106 and PC 107 "Other Terminals")). We find that Murakawa's network system allows for PC 101 and another terminal (e.g., PC 106 or PC 107) to communicate securely via security gateway 103. Ex. 1005, 1:64–2:4, Fig. 5; Pet. 24–25.

Lastly, we are not persuaded by Patent Owner's arguments that "[i]ncorporating Murakawa's security gateway 103 into Ishiyama does not fill in the missing limitation of the '[an]other terminal' because no host computer has been incorporated from Murakawa." PO Resp. 49; *see also id.*

at 45 (explaining that the claim recites "another terminal" and "other terminal"). Put differently, Patent Owner argues that "Petitioner's modification of Ishiyama by Murakawa does not explain how the combination provides the recited 'other terminal.'" *Id.* (citing Ex. 2009 ¶¶ 143–144). To the contrary, Petitioner argues that "Murakawa describes the forwarding of messages at a security gateway located between a mobile terminal and other terminals." Pet. 24. Petitioner then proceeds to describe Murakawa's Figure 5, and to identify Murakawa's PC 106 and PC 107 as other terminals. *See id.* at 24–25 (citing Ex. 1005, 1:59–63; annotating Ex. 1005, Fig. 5 (labeling PC 106 and PC 107 "Other Terminals")). Thus, we disagree with Patent Owner that "no host computer has been incorporated from Murakawa." PO Resp. 49.

In summary, we find combining Ishiyama's mobile address changing functionality with Murakawa's security gateway and another terminal teaches "[a] method for ensuring secure forwarding of a message in a telecommunication network, having at least one mobile terminal and another terminal and a security gateway therebetween."

2. *Establishing a Secure Connection*

Claim 1 further recites "establishing a secure connection having a first address of the mobile terminal as a first end-point and a gateway address of the security gateway as a second end-point." Ex. 1001, 10:54–56. We agree with Petitioner that the combination of Ishiyama and Murakawa teaches this limitation. Pet. 26–30. We find that Ishiyama teaches that mobile computer 2 first establishes an IPSec tunnel between its first address (CoA1) and correspondent host 3's address (CN). Ex. 1004, 8:25–26, 8:36–38, 8:43–47, 8:50–53, 11:9–17, 12:3–5, Fig. 4; Pet. 26–27. Furthermore, Ishiyama teaches that the IPSec tunnel is defined by, *inter alia*, the addresses of mobile computer 2 and correspondent host 3. Ex. 1004, 12:9–12, 12:51–59; Figs. 9A, 9B; Pet. 28–29.

In addition, we agree with Petitioner and find that Murakawa teaches a security gateway. Ex. 1005, 1:59–2:4, 2:62–65, 4:13–16, Fig. 5; Pet. 18–19, 24–25 (citing Ex. 1005, Fig. 5) (annotating the figure with "Security Gateway"). Moreover, Murakawa teaches establishing a secure connection between a terminal (PC 101) and the security gateway. Ex. 1005, 1:61–63 ("[I]n order to perform the IPsec communication, VPN 108 is established between PC 101 and security gateway 103."), Fig. 5.

In summary, we find combining Ishiyama's mobile address changing functionality with Murakawa's security gateway and another terminal teaches "establishing a secure connection having a first address of the mobile terminal as a first end-point and a gateway address of the security gateway as a second end-point."

3. Mobile Terminal Changing Addresses

Claim 1 further recites "the mobile terminal changing from the first address to a second address." Ex. 1001, 10:57–58. We agree with Petitioner and find that Ishiyama teaches that after the IPSec tunnel has been established, Ishiyama's mobile computer 2 moves networks, moving from a first address (CoA1) to a second address (CoA2). *See, e.g.*, Ex. 1004, 8:55–57, Fig. 4; Pet. 30. This is depicted in Ishiyama's Figure 4, as annotated by Petitioner, where mobile terminal 2 moves from its first location (dashed red box corresponding to CoA1) to its second location (solid red box corresponding to CoA2). *See* Pet. 30 (annotating Ex. 1004, Fig. 4).

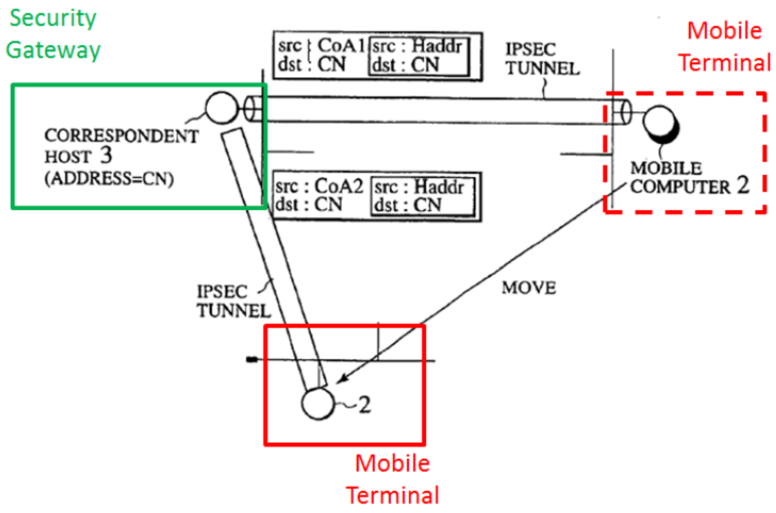
Based on Ishiyama's teachings, we find that the combination of Ishiyama and Murakawa teaches "the mobile terminal changing from the first address to a second address."

4. *While at the Second Address*

Claim 1 further recites "while at the second address, the mobile terminal sending a request message to the gateway address of the security gateway to request the security gateway to change the secure connection to be defined between the second address and the gateway address of the security gateway." Ex. 1001, 10:59–63. We agree with Petitioner that the combination of Ishiyama and Murakawa teaches this limitation. Pet. 31–33.

First, we agree with Petitioner and find that Ishiyama teaches that after a mobile terminal moves from a first address (CoA1) to a second address (CoA2), the mobile terminal sends a *request message* to the address of the correspondent host to change the security association definition from CoA1 to CoA2. Ex. 1004, 8:59–65; Pet. 31. Specifically, Ishiyama teaches that "the mobile computer 2 changes the source address of the outer packet of the encapsulated packet to be transmitted to the IPSEC tunnel by the mobile computer 2 into 'CoA2.'" Ex. 1004, 8:59–62; Pet. 31. We agree with Petitioner that Ishiyama teaches that "the encapsulated packet in which the outer packet has the source address ='CoA2' will be transferred." Ex. 1004, 8:63–65; Pet. 31. This is shown in Ishiyama's Figure 4, shown below as annotated in the Petition. *See* Pet. 31 (providing annotated Figure 4).

FIG. 4



Annotated Figure 4 "is a schematic diagram for explaining operations in the case where the mobile computer changes a connected location in the mobile communication system" with (i) a dotted-line red box around mobile computer 2 at its first location, (ii) a solid-line red box around mobile computer 2 at its second location, (iii) a solid-line green box around correspondent host 3, (iv) a "Mobile Terminal" label for each mobile computer 2 location, and (v) a "Security Gateway" label for correspondent host 3. Ex. 1004, 5:11–13; Pet. 31 (annotating Ex. 1004, Fig. 4). Ishiyama's Figure 4 illustrates that after the mobile computer 2 moves to a second address, a request message is sent from mobile computer 2 to correspondent host 3, with the request message illustrated as a rectangle (with "src: Haddr" and "dst: CN" labels) depicting the encapsulated packet, surrounded by a larger rectangle, depicting the outer packet (with "src: CoA2" and "dst: CN" labels). Ex. 1004, Fig. 4, 8:59–65; Pet. 35–36. Thus, Ishiyama teaches the entire transmitted packet comprises the request message. *Id.* at 8:59–65, Fig. 4. This finding is consistent with Petitioner's arguments made during the oral hearing that Ishiyama's entire transmitted packet (i.e., the encapsulated packet plus the outer packet, which has the changed source address) is the claimed request message. *See, e.g.*, Tr. 27:23–28:4, 29:10–17, 30:3–11, 34:14–35:1, 40:12–14, 65:8–67:7.

Second, we agree with Petitioner and find that Ishiyama teaches that the "[r]equest [is] for changing the security association to the correspondent [host]" as part of mobile computer 2 performing a SA Gateway Update. Pet. 32 (quoting Ex. 1004, 11:39–40); Ex. 1004, 11:39–46. More specifically, Ishiyama teaches that mobile computer 2's "request [is] to change the previous CoA used as the destination in the security association into the current CoA." Ex. 1004, 11:43–45; *see also* Pet. at 32 (annotating Ex. 1004, Fig. 7; citing Ex. 1004, 12:54–57 (arguing that "[t]he SA Gateway Update operation is depicted as operation (5) in Figure 7")). In other words, Ishiyama teaches that the request message is sent to request that the correspondent host change the secure connection so as to be defined between the mobile computer's second address and the address of the correspondent host. *See, e.g.*, Ex. 1004, 11:39–45, 12:54–60, Fig 7; Pet. 32. "As a result of these operations, at the correspondent [node] currently communicating with the mobile computer 2, the endpoint of the IPSEC tunnel is changed from 'CoA1' to 'CoA2' as the destination of all the security associations is changed to the current CoA 'CoA2.'" Ex. 1004, 12:66–13:3; Pet. 33.

In addition, as we discuss in detail above, Murakawa teaches a security gateway, as well as establishing a secure connection between a terminal (PC 101) and the security gateway. *See, e.g.*, Ex. 1005, 1:59–2:4, 2:62–65, 4:13–16, Fig. 5; *supra* Section VI(C)(1)–(2) (discussing our findings regarding, *inter alia*, Figure 5's teachings).

We find combining Ishiyama's mobile address changing functionality with Murakawa's security gateway and another terminal teaches "while at the second address, the mobile terminal sending a request message to the gateway address of the security gateway to request the security gateway to change the secure connection to be defined between the second address and the gateway address of the security gateway."

5. *In Response to the Request Message*

Claim 1 further recites "in response to the request message from the mobile terminal, the security gateway changing an address definition of the secure connection from the first address to the second address." Ex. 1001, 10:64–67. We agree with Petitioner and find that the combination of Ishiyama and Murakawa teaches this limitation. Pet. 33–34. We find that Ishiyama teaches that correspondent host 3 detects mobile computer 2's address change based on the request message (i.e., the source address in the request message's outer packet has changed), and updates mobile computer 2's address to CoA2 for the IPSec tunnel in the correspondent host's SA database. *See* Ex. 1004, 8:66–9:4, 12:51–59, Figs. 9B, 9D (illustrating exemplary SA databases); Pet. 33–34. Ishiyama's Figure 9B (mobile computer's first location) and Figure 9D (mobile computer's second location) illustrate this update at the correspondent host (labeled "CN" in the figures) by replacing Figure 9B's "dst" field value of "CoA1" with "CoA2," as shown in Figure 9D. *Compare* Ex. 1004, Fig. 9B, *with id.* at Fig. 9D. "As a result of these operations, at the correspondent [node] currently communicating with the mobile computer 2, the endpoint of the IPSEC tunnel is changed from 'CoA1' to 'CoA2' as the destination of all the security associations is changed to the current CoA 'CoA2'." Ex. 1004, 12:66–13:3; Pet. 34. In addition, as we discuss in detail above, Murakawa teaches a security gateway, as well as establishing a secure connection between a terminal and the security gateway. *See, e.g.*, Ex. 1005, 1:59–2:4, 2:62–65, 4:13–16, Fig. 5; *supra* Section VI(C)(1)–(2) (discussing our findings regarding, *inter alia*, Figure 5's teachings).

In summary, we find combining Ishiyama's mobile address changing functionality with Murakawa's security gateway and another terminal teaches "in response to the request message from the mobile terminal, the security gateway changing an address definition of the secure connection from the first address to the second address."

6. Mobile Terminal Sending a Secure Message

Claim 1 further recites "the mobile terminal sending a secure message in the secure connection from the second address of the mobile terminal to the other terminal via the security gateway." Ex. 1001, 11:1–3. We agree with Petitioner and find that the combination of Ishiyama and Murakawa teaches this limitation. Pet. 35–40. We find that Ishiyama teaches sending a secure message in the secure connection from the second address of Ishiyama's mobile computer to its correspondent host, as shown below in Figure 7's operation (6), as annotated by Petitioner. *See* Pet. 37 (annotating Ex. 1004, Fig. 7).

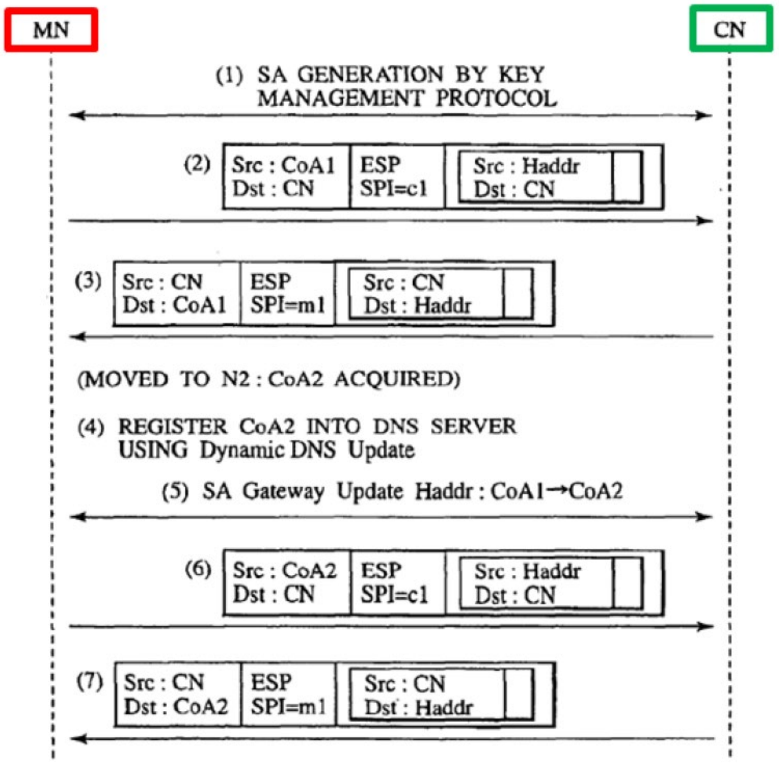
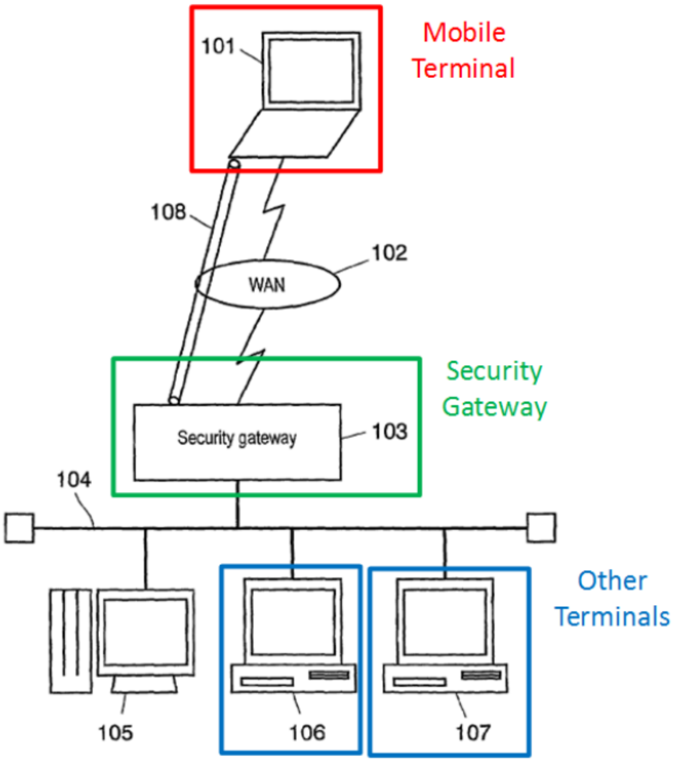

MN
CN
(1) SA GENERATION BY KEY MANAGEMENT PROTOCOL
(2) Src : CoA1 Dst : CN | ESP SPI=c1 | Src : Haddr Dst : CN
(3) Src : CN Dst : CoA1 | ESP SPI=m1 | Src : CN Dst : Haddr
(MOVED TO N2 : CoA2 ACQUIRED)
(4) REGISTER CoA2 INTO DNS SERVER USING Dynamic DNS Update
(5) SA Gateway Update Haddr : CoA1→CoA2
(6) Src : CoA2 Dst : CN | ESP SPI=c1 | Src : Haddr Dst : CN
(7) Src : CN Dst : CoA2 | ESP SPI=m1 | Src : CN Dst : Haddr

Figure 7 "is a sequence chart showing an exemplary processing sequence in the case where the mobile computer initiates communications at a visited site and then changes . . . location." Ex. 1004, 5:20–23. Petitioner annotated Figure 7 with a green box around the correspondent node ("CN") identifier and a red box around the mobile computer identifier ("MN"). Pet. 49 (annotating Ex. 1004, Fig. 7). Ishiyama teaches that as a result of its CoA update operations, "at the correspondent [host] currently communicating with the mobile computer 2, the endpoint of the IPSEC tunnel is changed from 'CoA1' to 'CoA2' as the destination of all the security associations,'" and "[c]onsequently, the session is guaranteed even when the mobile computer 2 moves . . . ." Ex. 1004, 12:66–13:5; Pet. 35 & n.6. Put differently, as Figure 7 illustrates, mobile computer 2 sends a secure message from its second address to correspondent host 3 using the same IPSec. Ex. 1004, Fig. 7 (illustrating for operation (6) that the outer packet's Src: has the value "CoA2" and Dst: has the value "CN"); 12:66–13:5.

As to Murakawa, we agree with Petitioner and find that Murakawa teaches a terminal sending a secure message in a secure connection to an address of another terminal via the security gateway. *E.g.*, Ex. 1005, Fig. 5; Pet. 38–39. This is shown in Murakawa's Figure 5, shown below as annotated in the Petition. *See* Pet. 38 (providing annotated Figure 5).

FIG. 5 PRIOR ART



Murakawa's Figure 5 shows a "prior art typical network system." Ex. 1005, 4:32–33. Petitioner annotated the figure with (i) a red box around PC 101 and labeled "Mobile Terminal," (ii) a green box around security gateway 103 and labeled "Security Gateway," and (iii) a blue box around each of PC 106 and PC 107, and labeled "Other Terminals." Pet. 38 (annotating Ex. 1005, Fig. 5). As illustrated in Figure 5, Murakawa teaches that outside terminal (PC 101) sends a secure message in the secure connection (VPN 108) to another terminal (PC 106) via security gateway 103. *Id.* at 1:61–2:4, 2:62–65, Fig. 5; *see also supra* Section VI(C)(1) (discussing our findings regarding Figure 5's teachings); Pet. 38–39.

Furthermore, we credit Dr. Goldschlag's testimony that one of ordinary skill in the art would have understood that Murakawa teaches a well-known IPSec tunnel mode configuration with a security gateway facilitating communication between a mobile terminal and other terminals because this testimony is consistent with our findings of Murakawa's teachings. *See* Ex. 1002 ¶¶ 85–88.

Accordingly, we find that the combination of Ishiyama and Murakawa teaches the mobile terminal sending a secure message in the secure connection (VPN 108) from its second address (CoA2) to the other terminal (PC 106) via security gateway 103.

Lastly, we are not persuaded by Patent Owner's arguments that Ishiyama's "operation (6) is shown to be an end-to-end, two-way secure communication from the mobile terminal MN to the correspondent terminal CN," and does not teach "[t]he three-component connection called for by the claim (mobile terminal-security gateway-other terminal)." PO Resp. 57. Patent Owner focuses on Ishiyama's teachings individually, rather than the combined teachings of Ishiyama and Murakawa. *See In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986) ("Non-obviousness cannot be established by attacking references individually where the rejection is based upon the teachings of a combination of references"). Again, as to the second way Petitioner combines Ishiyama and Murakawa, Ishiyama's mobile address changing functionality is combined with Murakawa's security gateway configuration (e.g., security gateway 103 and other terminal 106). *See* Pet. 12–54; Dec. on Inst. 24–25, 37–38 (noting the two alternative ways). Hence, a mobile terminal securely communicates with another terminal via Murakawa's security gateway 103 rather than Ishiyama's correspondent host 3. *Id.*

In summary, we find combining Ishiyama's mobile address changing functionality with Murakawa's security gateway and another terminal teaches "the mobile terminal sending a secure message in the secure connection from the second address of the mobile terminal to the other terminal via the security gateway."

7. *Combining Ishiyama and Murakawa*

For the reasons we provide below, we find that Petitioner has demonstrated by a preponderance of the evidence that one of ordinary skill in the art would have found it obvious to combine Ishiyama's mobile address changing functionality with Murakawa's security gateway and other terminal in the manner claimed.

First, we agree with Petitioner and find that Ishiyama teaches using IPSec in tunnel mode with its mobile address changing functionality. *E.g.*, Ex. 1004, 7:45–49, 8:43–65, 11:9–16, Fig. 4; Pet. 17–18, 20, 22. More specifically, we find that Ishiyama teaches that "mobile computer 2 always uses the IPSEC in the tunnel mode at a time of making a connection to the correspondent host 3." Ex. 1004, 11:9–16. Figure 4 also illustrates that mobile computer 2 connects to correspondent host 3 via an IPSec tunnel. *See* Ex. 1004, Fig. 4 (labeling the connections as "IPSEC TUNNEL"), 8:43–65; Pet. 22.

Second, Petitioner persuasively shows that one of ordinary skill in the art would have understood that tunnel mode was used for communicating via a security gateway. Specifically, we find that one of ordinary skill in the art would have known that "[t]unnel mode . . . is generally used for sending messages through more than two components . . . ." Ex. 1001, 3:19–21[9]; Pet. 17 (citing Ex. 1001, 3:19–30; Ex. 1002 ¶ 57). We also credit in support of this finding the below deposition testimony of Patent Owner's expert, Dr. Rouskas, who testified as follows:

> Q: So in all the instances where you personally have used IPSec, you have only ever used IPSec tunnel mode with security gateway being one of the endpoints. Right?
>
> A: So I have been using IPSec for, you know, more than 20 years. But to the best of my recollection that is right, I have only used it when one of endpoints is security gateway.

[9] "Statements in a challenged patent's specification may be used . . . when they evidence the general knowledge possessed by someone of ordinary skill in the art." Memorandum: Treatment of Statements of the Applicant in the Challenged Patent in Inter Partes Reviews Under § 311 (Aug. 2020) (available at https://www.uspto.gov/sites/default/files/documents/signed_aapa_guidance_memo.pdf), 4. "Permissible uses . . . under § 103 include . . . supporting a motivation to combine particular disclosures." *Id.* at 6 (citing *Koninklijke Philips v. Google*, 948 F.3d 1330, 1337–38 (Fed. Cir. 2020)). We find that the statements cited by Petitioner from the '581 patent's Technical Background section evidence the general knowledge possessed by one of ordinary skill in the art at the time of the invention of the '581 patent as they are contained in the "Technical Background" section and are consistent with the evidence of record. *See, e.g.*, Pet. 8–9 (citing, e.g., Ex. 1001, 3:10–11, 3:14–15, 3:22–24), 17 (citing Ex. 1001, 3:19–30), 20 (citing Ex. 1001, 3:19–21). Patent Owner does not challenge Petitioner's reliance on statements from the Technical Background section of the '581 patent. *See generally* PO Resp. Even so, we reach the same conclusions even without reliance on the statements from the '581 patent.

Ex. 1019, 111:21–112:9; Pet. Reply 8. In addition, we credit Dr. Goldschlag's declaration testimony, which is consistent with contemporaneous evidence in the record, that "[t]unnel mode is used when one or both ends of an SA is a security gateway . . . that implements IPSec." Ex. 1002 ¶ 33 (quoting Ex. 1009, 14) (emphasis omitted); *see also* Ex. 1001, 3:19–21 (admitting that "tunnel mode is often used when one or both ends of a SA is a security gateway, such as a firewall or router that implements IPSec"); Pet. 20.

Lastly, we agree with Petitioner and find that tunneling packets through a security gateway for two terminals to communicate (such as in Murakawa) was well-known in the art at the time of the invention of the '581 patent. Pet. 24–25. In particular, we find that Murakawa's security gateway configuration (e.g., Figure 5) is "a prior art typical network system," which provides communications between terminals. Ex. 1005, 4:32–33, Fig. 5; Pet. 24–25. Moreover, in its Technical Background section, the '581 patent teaches the following:

> The IPSec tunnel mode operates e.g. in such a way that if a host on a network generates an IP packet with a destination address of another host on another network, the packet is routed from the originating host to a security gateway (SGW), firewall or other secure router at the boundary of the first network. The SGW or the like filters all outgoing packets to determine the need for IPSec processing. If this packet from the first host to another host requires IPSec, the firewall performs IPSec processing and encapsulates the packet in an outer IP header. The source IP address of this outer IP header is this firewall and the destination address may be a firewall that forms the boundary to the other local network. This packet is now routed to the other host[']s firewall with intermediate routers examining only the outer IP header. At the other host firewall, the outer IP header is stripped off and the inner packet is delivered to the other host.

Ex. 1001, 3:47–62; *see also* Pet. 36, 43. In other words, this passage also teaches that tunneling packets through a security gateway for two terminals to communicate was well-known in the art at the time of the invention of the ’581 patent. Ex. 1001, 3:47–62. We also credit Dr. Goldschlag’s testimony that it was well-known in the art for a security gateway, such as that disclosed in Murakawa, to facilitate communication between a mobile terminal and other terminals as this testimony is consistent with Murakawa’s teachings. Ex. 1002 ¶ 66; Pet. 24.

In summary, we find that (1) Ishiyama’s address changing functionality employs tunnel mode, (2) tunnel mode was generally used when at least one end of an SA was a security gateway, and (3) Murakawa teaches a typical, prior art security gateway configuration. Based on these findings, we find that one of ordinary skill in the art would have found it obvious to employ Ishiyama’s address changing functionality with a security gateway, such as taught in Murakawa. *See PGS Geophysical AS v. Iancu*, 891 F.3d 1354, 1365 (Fed. Cir. 2018) (“[T]he motivation to modify a reference can come from the knowledge of those skilled in the art, from the prior art reference itself, or from the nature of the problem to be solved.”) (citation omitted).

Put differently, based on these findings, Ishiyama’s use of tunnel mode would have suggested to one of ordinary skill in the art using Ishiyama’s address changing functionality with Murakawa’s security gateway configuration. *Id.*; Pet. 18, 20, 22, 23, 25. We also credit Dr. Goldschlag’s testimony that one of ordinary skill in the art “reading Ishiyama would have understood that the use of tunnel mode suggests the use of a security gateway that tunnels messages to an ‘other node.’”

Ex. 1002 ¶ 61 (citing *id.* ¶¶ 33–36); Pet. 20. This testimony is consistent with our findings discussed above.

Additionally, we also credit the following testimony of Dr. Goldschlag:

> [I]n view of Ishiyama's stated goal of addressing a mobile terminal with a changing address, [one of ordinary skill in the art] would have understood that implementing Ishiyama's correspondent host functionality with the security gateway described in Murakawa would be highly desirable in the telecommunication context. As Ishiyama explains, implementing its IPsec address updating algorithm allows a mobile terminal and a security gateway to maintain communication 'without interrupting the session' initially established even when the mobile terminal changes to another address.

Ex. 1002 ¶ 68 (citing Ex. 1004, 6:54–60); Pet. 25. We find that one of ordinary skill in the art would have been motivated to incorporate Ishiyama's mobile address changing functionality with Murakawa's security gateway configuration "to maintain communication 'without interrupting the session' initially established even when the mobile terminal changes to another address." Ex. 1002 ¶ 68; *KSR*, 550 U.S. 417 ("[I]f a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious . . . ."). Moreover, we do not find this testimony conclusory, as Patent Owner alleges (PO Resp. 50), because Dr. Goldschlag explains why combining Ishiyama and Murakawa would have been highly desirable (i.e., because it would maintain communication without interrupting the session). Ex. 1002 ¶ 68 (citing Ex. 1004, 6:54–60). We agree that having no interruption when the mobile terminal moves "would [have] be[en] highly desirable in the telecommunication context." *Id.*

We are not persuaded by Patent Owner's arguments that Petitioner "fails to provide the requisite explanation as to **how** Ishiyama and Murakawa are to be combined or **what is the operation of the resulting combination**." PO Resp. 51; *see also id.* at 59 (citing Ex. 2009 ¶ 152). Rather, we agree with Petitioner and find that one of ordinary skill in the art "could[10] have easily performed th[e] implementation" of combining Ishiyama's address changing functionality with the security gateway described in Murakawa "in view of the security gateway suggestion from Ishiyama's tunnel mode operation." Pet. 26 (citing Ex. 1002 ¶ 69). Simply put, Ishiyama's mobile computer 2 communicates with correspondent host 3 using IPSec tunnel mode just as Murakawa's PC 101 communicates with security gateway 103 using IPSec tunnel mode. *E.g.*, Ex. 1004, 8:43–49, 11:9–16, Fig. 4; Ex. 1005, 1:61–63, 2:62–65, Fig. 5; Pet. 39. Ishiyama's address changing functionality utilizes the outer packet's source address with Ishiyama's tunnel mode connection. *E.g.*, 1004, 8:43–65, Fig. 4. Petitioner's combination likewise utilizes the outer packet's source address (as in Ishiyama) with Murakawa's tunnel mode connection. *E.g.*, 1004,

[10] Although we consider whether one of ordinary skill in the art "could" have combined Ishiyama's and Murakawa's relevant teachings with respect to these arguments related to operability, we above find that one of ordinary skill in the art "would" have combined Ishiyama's and Murakawa's relevant teachings. *See PGS Geophysical*, 891 F.3d at 1365 (recognizing that whether one of ordinary skill in the art "could" or "would" have combined references are related, separate questions); *see also supra* Section VI(C)(7) (finding that one of ordinary skill in the art would have combined the references).

8:43–65, Fig. 4.; Ex. 1005, 1:59–2:4, Fig. 5; Pet. 38–40; Pet. Reply 16–17 (citing Pet. 39–40; Ex. 1022 ¶¶ 48–56). Moreover, we do not find Dr. Goldschlag's testimony conclusory, as Patent Owner alleges (PO Resp. 59), but rather Dr. Goldschlag explains that one of ordinary skill in the art could have easily combined Ishiyama's address changing functionality with the security gateway described in Murakawa in light of Ishiyama's tunnel mode operation (i.e., both Murakawa and Ishiyama employ tunnel mode). *See* Ex. 1002 ¶ 68.

We also are not persuaded by Patent Owner's argument that "the security gateway 103 and computer 106 illustrated in Murakawa's Figure 5 could not be combined into the address changing system as of Ishiyama illustrated in Figure 4." PO Resp. 53. In particular, Patent Owner argues "that Ishiyama's security policy databases [("SPDs")] (Figures 8A–8B) and the security association databases [("SADs")] (Figures 9A–9D) would not operate if the components of Murakawa were inserted in place of Ishiyama's correspondent host." *Id.* at 53–54 (citing Ex. 2009 ¶ 148). Contrary to Patent Owner's arguments, however, "it is not necessary that the inventions of the references be physically combinable to render obvious the invention under review." *In re Sneed*, 710 F.2d 1544, 1550 (Fed. Cir. 1983). The relevant inquiry is whether the claimed subject matter would have been obvious to those of ordinary skill in the art in light of the combined teachings of those references. *See In re Keller*, 642 F.2d 413, 425 (CCPA 1981). And, as we find above, one of ordinary skill in the art would have found it obvious to combine Ishiyama's address changing functionality with Murakawa's security gateway and other terminal. This does not mean that Ishiyama's specific SPD and SAD databases are used in that combination, as

Patent Owner argues. *In re Nievelt*, 482 F.2d 965, 968 (CCPA 1973) ("Combining the *teachings* of references does not involve an ability to combine their specific structures."); *see also In re Mouttet*, 686 F.3d 1322, 1332 (Fed. Cir. 2012) ("It is well-established that a determination of obviousness based on teachings from multiple references does not require an actual, physical substitution of elements." (citing *In re Etter*, 756 F.2d 852, 859 (Fed. Cir. 1985) (en banc))). Rather, one of ordinary skill in the art would have "be[en] able to fit the teachings of [Ishiyama and Murakawa] . . . together like pieces of a puzzle" because the skilled artisan is "a person of ordinary creativity, not an automaton." *KSR*, 550 U.S. at 420–21. Likewise, we are not persuaded by Patent Owner's example that if a new terminal with a new address was added, "the Ishiyama system would be unable to process messages sent to or received from the new terminal" because the new address would not be found in Ishiyama's SPD. PO Resp. 53. Again, combining the teachings of Ishiyama and Murakawa does not involve woodenly combining their specific structures, and does not require using Ishiyama's specific SPD. *Nievelt*, 482 F.2d at 968. And, Murakawa's existing role in addressing packets between terminals (e.g., PC 101 and PC 106) also remains a part of Petitioner's combination. *See, e.g.*, *infra* Section VI(G) (discussing Murakawa's Figure 8, and accompanying text, concerning addressing messages sent between terminals via a security gateway); Pet. 45.

Likewise, we are not persuaded by Patent Owner's argument that "Petitioner fails to explain what modifications to Ishiyama's . . . [SPDs and SADs] would be required for Ishiyama to work with security gateway 103 as the opposing endpoint instead of correspondent host 3." PO Sur-Reply 20 (citing Ex. 1004, Figs. 8–9). Again, Ishiyama's specific SPDs and SADs are not part of Petitioner's combination. *In re Nievelt*, 482 F.2d at 968. In addition, we agree with Petitioner and find that SADs and SPDs are commonplace in IPSec communications, and security gateways are required to have at least "one pair of SADs and one pair of SPDs." *See* Pet. Reply 13 (citing Ex. 1011, 13; Ex. 1019, 89:8–15); *see also* Ex. 1022 ¶ 56. And, we agree with Petitioner that Ishiyama's description of SPDs and SADs "does not preclude the operation of a security gateway also implementing these components." Pet. Reply 17 (citing Ex. 1022 ¶ 56). In other words, we find that one of ordinary skill in the art would have understood that the address changing functionality used with Ishiyama's SPDs and SADs also can be used with the SPDs and SADs of a common security gateway configuration, such as described by Murakawa. *See* Ex. 1011, 13; Ex. 1019, 89:8–15; Ex. 1022 ¶ 56. Accordingly, we find that one of ordinary skill in the art would have found it obvious to combine the teachings of Ishiyama and Murakawa to provide for Ishiyama's address changing functionality being incorporated into Murakawa's security gateway configuration. *See KSR*, 550 U.S. at 420–21 (finding the skilled artisan would "be able to fit the teachings of multiple patents together like pieces of a puzzle" because the skilled artisan is "a person of ordinary creativity, not an automaton"). In addition, we find misplaced Patent Owner's focus on Petitioner's use of the word "preclude." PO Sur-Reply 18 (arguing that Ishiyama "should be interpreted for what it affirmatively teaches as opposed to what it does not 'preclude'") (citation omitted). In the context of Petitioner's argument, it is clear that Petitioner means that Murakawa's security gateway's SPDs and SADs also can implement Ishiyama's address changing functionality. *See* Pet. Reply 17 (citing Ex. 1022 ¶ 56).

We also are not persuaded by Patent Owner's argument that "[a] person of ordinary skill in the art would not readily understand how Ishiyama's SA databases could be modified to accommodate Murakawa's components." PO Resp. 53 (citing Ex. 2009 ¶ 148). Nor are we persuaded that "[a] person of ordinary skill would not have a reasonable expectation of success given that there is no explanation as to how the references would be combined and how the resulting system would operate," as Patent Owner argues. *Id.* (citation omitted). Rather, as we find above, combining the teachings of Ishiyama and Murakawa does not require using Ishiyama's specific SA databases. *Nievelt*, 482 F.2d at 968. And, as we find above, one of ordinary skill in the art would and could have easily combined Ishiyama's address changing functionality with the security gateway described in Murakawa. *See* Ex. 1002 ¶ 68.

We also are not persuaded by Patent Owner's argument that "a person of ordinary skill would be taught away from combining Ishiyama and Murakawa." PO Resp. 54. We find that Patent Owner does not cite any portion of Ishiyama that criticizes, discredits, or otherwise discourages combining Ishiyama's mobile address changing functionality with Murakawa's security gateway configuration. *Id.*; *In re Fulton*, 391 F.3d 1195, 1201 (Fed. Cir. 2004) (teaching away requires that a reference "criticize, discredit, or otherwise discourage" investigation into the claimed solution). To the contrary, as we find above, Ishiyama's use of tunnel mode suggests combining its address changing functionality with Murakawa's security gateway configuration. *In re Urbanski*, 809 F.3d 1237, 1243–44 (Fed. Cir. 2016) (finding that there was no teaching away as the prior art references suggested the modification and did not teach that the modified process would be inoperable). We also do not credit Dr. Rouskas' testimony as it is contrary to our findings above. Ex. 2009 ¶ 148.

Lastly, we agree with Patent Owner that only asserting that references "could" be combined may be insufficient. PO Resp. 52–53 (citations omitted). However, as we find above, Petitioner provides persuasive articulated reasoning as to why one of ordinary skill in the art "would" have combined Ishiyama's address changing functionality with Murakawa's security gateway configuration. Thus, we are not persuaded that Petitioner fails to show sufficient rationale for combining Ishiyama and Murakawa.

Accordingly, for the reasons discussed above, we find that Petitioner provides "some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *See In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006) (citations omitted), *cited with approval in KSR*, 550 U.S. at 418.

8. *Alleged Security Flaw*

Patent Owner argues in its Sur-Reply[11] that there is "a major security flaw in Ishiyama that would prevent it from ever being used by . . . [one of ordinary skill in the art] as a reference to construct a secure communication system." PO Sur-Reply 1. In particular, Patent Owner argues that "the new

[11] Petitioner sought our authorization to file a motion to strike Patent Owner's Sur-Reply, or, in the alternative, to file a Sur-Sur-Reply to address the new security flaw argument. Paper 34, 2. We denied the request, finding that, as in most cases, we are "capable of identifying new issues . . . when weighing the evidence at the close of trial, and disregarding any new issues . . . that exceeds the proper scope of . . . sur-reply." *Id.* at 3 (quoting Patent Trial and Appeal Board Consolidated Trial Practice Guide 80 ("Consolidated Practice Guide") (Nov. 2019) (available at https://www.uspto.gov/TrialPracticeGuideConsolidated)).

source address in the outer packet of Ishiyama's . . . request message . . . is unencrypted and sent in the clear." *Id.* Because of this flaw, one of ordinary skill in the art "would never use Ishiyama's outer packet to change the address definition for the mobile device in a secure connection because it could easily be intercepted by a malicious intermediary and manipulated to cause message traffic to be misdirected to an imposter device," according to Patent Owner. *Id.*; *see also id.* at 2–11 (arguing Ishiyama's security flaw defeats Petitioner's unpatentability allegations).

The security flaw argument, however, is new. Nowhere in its Response does Patent Owner make this argument. *See generally* PO Resp.; *see also* Tr. 48:11–25 (Patent Owner admitting that it did not address the security flaw issue in its Response). Furthermore, Patent Owner admits that "[n]either the Reply nor [Petitioner's] expert's supplemental declaration address the security flaw." PO Sur-Reply 5 n.1 (citing Ex. 1022). Accordingly, we do not consider Patent Owner's security flaw argument because it was not made in the Patent Owner Response and is beyond the proper scope of the Sur-Reply, and thus, is waived. *See* Paper 11 (Scheduling Order), 7 ("Patent Owner is cautioned that any arguments for patentability not raised in the response may be deemed waived."); Consolidated Practice Guide 74 (citing 37 C.F.R. § 42.23) ("Generally, a reply or sur-reply may only respond to arguments raised in the preceding brief.").

Additionally, we are not persuaded by Patent Owner's arguments to excuse the waiver.[12] During the oral hearing, Patent Owner argued that the Petition was unclear as to whether the request message was (i) "the message containing the outer header where the source address of the outer header has been changed from CoA1 to CoA2," as shown in Figure 4 of Ishiyama, or (2) "step 5, the SA gateway update operation, of Figure 7 of Ishiyama." Tr. 47:2–14. Patent Owner argued that it asked Dr. Goldschlag during his deposition "to elaborate on what [Petitioner]'s position was as to what was the claim's request message." *Id.* at 45:2–4. According to Patent Owner, "Dr. Goldschlag clarified that the claimed request message was step 5 of Figure 7 at the Ishiyama patent," and not the outer header. *Id.* at 45:4–6, 48:19–49:10. Patent Owner argued that it did not address the security flaw argument in its Response[13] based on (i) the Petition not clearly identifying that the request message includes the outer header, and (ii) Patent Owner's "reliance on Dr. Goldschlag's testimony that the request message was step 5 and not the outer header." *Id.* at 48:19–49:10.

We are not persuaded by Patent Owner's arguments for either reason. First, as we discuss above, the Petition clearly sets forth that Ishiyama's request message includes the outer packet's source address. *See supra* Section VI(C)(4) (addressing, *inter alia*, Ishiyama's Figure 4 and accompanying text). For example, the Petition states:

[12] We are not suggesting that providing reasons during the oral hearing for why a new argument was made in a Sur-Reply is the appropriate procedural mechanism, if any, to excuse waiver. Regardless, we address the merits of Patent Owner's reasons here.

[13] Patent Owner argued that it included its security flaw argument in its Sur-Reply in light of Petitioner's Reply, which explains that the request message includes the outer packet. Tr. 47:18–48:7.

> After the mobile terminal of Ishiyama moves from CoA1 (i.e., *first* address) to CoA2 (i.e., *second* address), Ishiyama further describes the *sending a request message to the gateway address* of the correspondent node (i.e[.], *security gateway*) to change the security association definition from CoA1 to CoA2. This is shown below in Figure 4 (annotated). Specifically, "the mobile computer 2 changes the source address of the outer packet of the encapsulated packet to be transmitted to the IPSEC tunnel by the mobile computer 2 into 'CoA2'. . . . [T]he encapsulated packet in which the outer packet has the source address ='CoA2' will be transferred." Ishiyama, 8:59–65.

Pet. 31. Moreover, in our Decision on Institution, when addressing the claimed request message, we noted that:

> Petitioner argues that after changing addresses, mobile computer 2 sends a message (*having CoA2 for its outer packet's source address*) to correspondent host 3 via the IPSec tunnel, requesting that correspondent host 3 update to mobile computer 2's new address. [Pet. 31–33] (citing Ex. 1004, 8:59–65, 11:39–45, 12:66–13:5, Figs. 4, 7).

Dec. on Inst. 31 (emphasis added). Accordingly, we find that the Petition clearly sets forth that Ishiyama's request message includes the outer packet's source address.

Second, we disagree with Patent Owner that Dr. Goldschlag testified that "the request message is step 5 of Figure 7, *not the outer header of the message in Figure 4*." Tr. 45:10–13 (emphasis added). In support of its argument, Patent Owner referenced the following deposition testimony during the oral hearing:

> Q [D]o you recall that in the [P]etitioner's analysis of Claim 1, the recited request was allegedly satisfied by the SA gateway update Operation 5 in Figure 7 of Ishiyama?

> A Right. So I think that was the section that we were just looking through, that Paragraph 7[5] in my declaration[14] which walks through the address change operation.

Tr. 45:14–18 (quoting Ex. 2008, 219:12–19).[15] Patent Owner incorrectly focused on only the first word of Dr. Goldschlag's answer — "Right." *Id.* at 45:10–18. Dr. Goldschlag clearly includes paragraph 75 of his declaration in his answer to the question. *Id.* Paragraph 75, *inter alia*, annotates Figure 4 and states that it "depicts the change in the security association definition from CoA1 to CoA2." Ex. 1002 ¶ 75 (citing Ex. 1004, 8:59–65; annotating Ex. 1004, Fig. 4). Thus, this deposition testimony clearly does not support that Dr. Goldschlag testified that the request message does not include the outer header of the message or Figure 4's teachings.

Patent Owner also cited additional deposition testimony of Dr. Goldschlag during the oral hearing in support of its argument. Tr. 45:7–

[14] Dr. Goldschlag was referring to his declaration submitted in IPR2019-00819 (Ex. 1002), as Patent Owner had previously marked that declaration during the deposition, placed it before Dr. Goldschlag, and questioned him on it. Ex. 2008, 20:17–20, 189:15–19, 209:22–217:10. Dr. Goldschlag's declaration in IPR2019-00820 (Ex. 1002) was marked by Patent Owner later in the deposition. *Id.* at 233:1–2, 233:10–13. This timing applies to all of Dr. Goldschlag's deposition testimony discussed in this section. Moreover, paragraphs 74–76 of the IPR2019-00819 declaration appear in the IPR2019-00820 declaration, but shifted by one paragraph number (i.e., 74–76 correspond to 75–77). We adjust the numbering in Dr. Goldschlag's testimony for clarity to refer to the correct paragraph in the IPR2019-00820 declaration.

[15] During the oral hearing, Patent Owner read this question and the first word ("Right.") of Dr. Goldschlag's answer into the record, rather than providing the specific cite. Tr. 45:14–18. We here provide Dr. Goldschlag's complete answer to the question posed.

10 (citing Ex. 2008, 219:20–220:4, 228:1–9). For example, Patent Owner identified the following testimony:

> Q So is it correct that the request recited in the claim is alleged to correspond to the SA update -- SA gateway update operation, Step 5 of Figure 7 of Ishiyama?
> I can refer you to the petition.
> A Right. So the SA update operation is in Operation 5 --
> Q Okay.
> A -- and that's Paragraph 7[7] of my declaration.

Ex. 2008, 219:20–220:6.[16] This passage supports that operation 5 of Figure 7 teaches about the claimed request message, as cited in the Petition. *See id.*; Pet. 36–37. It does not exclude, however, the teachings of Figure 4, and its accompanying text. *See* Ex. 2008, 219:20–220:6. "F[igure] 4 is a schematic diagram for explaining operations in the case where the mobile computer changes a connected location in the mobile communication system of F[igure] 2" while "F[igure] 7 is a sequence chart showing an exemplary processing sequence in the case where the mobile computer initiates communications at a visited site and then changes a location in the mobile communication system of F[igure] 2." *Compare* Ex. 1004, 5:11–13, *with id.* at 5:21–24. In other words, Figure 4 and Figure 7 are not mutually exclusive, but rather are complementary in teaching Ishiyama's invention. *Id.* Petitioner cites both figures in support of its arguments that Ishiyama teaches the claimed request message. Pet. 35–37.

Moreover, paragraph 77 of Dr. Goldschlag's declaration (to which he refers in his answer) begins "Ishiyama refers to this operation as an 'SA Gateway Update,'" referring to the previous declaration paragraph 76.

[16] Patent Owner cited only a portion of Dr. Goldschlag's answer (through line 4) to the question posed, but we here provide his answer in its entirety.

Ex. 1002 ¶ 77. Paragraph 76 recites that "the mobile computer 2 changes the source address of the outer packet of the encapsulated packet to be transmitted to the IPSEC tunnel by the mobile computer 2 into 'CoA2'" and that "the encapsulated packet in which the outer packet has the source address ='CoA2' will be transferred." Ex. 1002 ¶ 76 (citing Ex. 1004, 8:59–65). Thus, this deposition testimony clearly does not exclude the outer packet from the request message. Ex. 2008, 219:20–220:6. Likewise, the third passage of deposition testimony cited by Patent Owner does not exclude the outer header from the request message, but simply discusses Figure 7's teachings. Ex. 2008, 228:1–9.

Lastly, we provide the following example from Dr. Goldschlag's deposition testimony, which Patent Owner did not cite during the oral hearing but which provides further context for the cited testimony, where Dr. Goldschlag testified that the request message included the teachings of Figure 4.

> Q And in the claim, it indicates that the request is sent from the mobile terminal to the security gateway, and you've mapped that to Operation 5 in Figure 7[?]
> A Which is also from the mobile terminal to the security gateway, right. And if you go back to it picture, right, there is that IPsec tunnel. If you go back to Figure 4, if you don't mind.
> Q Let's just stick with Figure 7, please.
> A But Figure 4 will help sort of illustrate it. The mobile computer has a tunnel, and one of the purposes of the change of address is to use the same SA for the new tunnel, so it uses the new tunnel and it sends those messages over that tunnel.

Ex. 2008, 229:19–230:10.

In summary, Dr. Goldschlag's deposition testimony, taken as a whole, does not support a finding that Dr. Goldschlag stated the request message excludes Figure 4's teachings and the use of the outer header's source address. Ex. 2008, 219:12–220:6, 228:1–9.

Additionally, we are not persuaded by Patent Owner's argument that "Petitioner was aware of the security flaw (see March 20, 2020, deposition of Dr. Rouskas) well in advance of the Reply (filed April 1, 2020)" and chose not to address it in its Reply. PO Sur-Reply 5 n.1; *see also* Tr. 49:24–50:6. Again, Patent Owner does not address the security flaw argument in its Response. *See generally* PO Resp. Thus, Petitioner correctly did not address the security flaw argument in its Reply because doing so would have been beyond the proper scope of the Reply. *See* 37 C.F.R. § 42.23(b) ("A reply may only respond to arguments raised in the corresponding . . . patent owner response."); Consolidated Practice Guide 74.

Lastly, Patent Owner certainly was aware of its security flaw argument at least as early as March 20, 2020 when Patent Owner's expert, Dr. Rouskas, was deposed. During this deposition, Patent Owner on redirect extensively questioned Dr. Rouskas on Ishiyama's alleged security flaw. *See* Ex. 1019, 184:6–197:22. This occurred more than ten days before Petitioner filed its Reply on April 1, 2020. Nonetheless, Patent Owner did not seek our authorization to supplement its Response (with a showing of good cause) during that more than ten day period or afterwards.

D. Challenged Claim 2

Claim 2 depends from independent claim 1, and recites "[t]he method of claim 1, wherein the secure connection is established in step a) by forming a Security Association (SA)." Ex. 1001, 11:4–5. Patent Owner does not raise any arguments specific to claim 2.

We agree with Petitioner and find that Ishiyama teaches this additional limitation. Pet. 47–48. We find that Ishiyama teaches that "mobile computer 2 always uses the IPSEC in the tunnel mode at a time of making a connection to the correspondent host 3, [and] the appropriate existing key management protocol is followed at a time of exchanging the *security association* with the correspondent host 3." Ex. 1004, 11:9–17 (emphasis added). Ishiyama also teaches that "a procedure for making agreement regarding the contents of the *security association* with the correspondent is carried out before the use of the IPSEC [tunnel]." *Id.* at 9:63–66 (emphasis added). And, Ishiyama teaches that its "IPSEC processing is carried out according to the contents described in the *security association*." *Id.* at 9:50–51 (emphasis added).

Accordingly, based on a review of the entire record, we find that Petitioner has demonstrated by a preponderance of the evidence that claim 2 would have been obvious over the combined teachings of Ishiyama and Murakawa.

E. Challenged Claim 4

Claim 4 depends from independent claim 1, and recites "[t]he method of claim 1, wherein the request message and/or a reply message is encrypted and/or authenticated." Ex. 1001, 11:9–10. Petitioner argues that Ishiyama teaches that the request message is encrypted. Pet. 48–50. We disagree.

Petitioner focuses on only a portion of Ishiyama's request message (i.e., the encapsulated packet) in arguing that Ishiyama teaches that the request message is encrypted. *See* Pet. 48–50; Pet. Reply 18–19. For example, Petitioner argues that "Ishiyama explains that the mobile computer 2 includes 'an encryption unit 114 for carrying out the encapsulation and encryption on transmission packets.'" Pet. 49 (quoting Ex. 1004, 13:40–41; citing Ex. 1004, 13:33–35). "Indeed a main requirement and pillar of IPsec is to encrypt messages," according to Petitioner. *Id.* (citing Ex. 1011, 4 at § 2.1, 6–7 at §§ 3.1–3.2). Moreover, Petitioner argues that "Ishiyama explains that '[i]n the tunnel mode IPSEC communications, the packet encapsulation and the encryption/decryption of the inner packet are carried out and the IPSEC module 22 [of mobile unit 2] has functions for realizing such encapsulation and encryption/decryption processing.'" Pet. Reply 18 (quoting Ex. 1004, 7:56–60). "The mobile unit then uses this IPSEC module to transmit an 'encapsulated packet' via the IPSEC tunnel to update the address at the other endpoint," according to Petitioner. *Id.* (citing Ex. 1004, 8:55–9:10). Petitioner argues that "[b]y using IPSec to perform the update, the packet and the request message are encrypted." *Id.* at 18–19 (citing Ex. 1022 ¶¶ 60–62; Ex. 1011, 4 at § 2.1, 6–7 at §§ 3.1–3.2). Petitioner adds that Patent Owner's expert, "Dr. Rouskas[,] even confirmed this during his deposition." *Id.* at 19 (citing Ex. 1019, 175:19–176:2 (Dr. Rouskas testifying "[s]o, yes, the payload of that packet is encrypted")).

None of the passages that Petitioner cites for this limitation, however, teach that the request message's outer packet's source address is encrypted. Rather, Ishiyama only teaches that the encapsulated packet (payload) is encrypted. *E.g.*, Ex. 1004, 7:56–60. In fact, Petitioner admits that in Ishiyama the request message's outer packet's source address is unencrypted. *See, e.g.*, Tr. 27:9–16. However, the outer packet's source address is a part of the request message in Ishiyama. *See, e.g.*, Ex. 1004, Fig. 4, 8:59–65. For example, Ishiyama teaches the following:

> [W]hen the current location address of the mobile computer is changed to a new address, the mobile computer notifies the change of the own current location address to the correspondent by setting the new current location address as the source address of the outer packet of the encapsulated packet. Upon receiving this encapsulated packet, the correspondent can continue communications by changing only the destination address of the outer packet to the new current location address in the encapsulated packets to be transmitted thereafter.

Id. at 6:13–22. Thus, Ishiyama describes the request message as including the outer packet, and that packet is unencrypted.

Claim 4 recites that "the request message . . . is encrypted." Ex. 1001, 11:9–10. Thus, the plain words of the claim state that the message is encrypted—not that a portion of the message is encrypted. The '581 patent Specification likewise does not describe that only a portion of the request message is encrypted. *Id.* at 9:60–10:5. Specifically, the Specification discloses that, "[i]n signal 10a of [Figure 5]," which is sent from the mobile terminal when a mobile terminal moves to address B, "a request for registration (RREQ) of the new address is sent." *Id.* at 9:63–66. The Specification adds that "signal[] 10a . . . can be encrypted and/or authenticated." *Id.* at 10:1–2. Petitioner does not identify any description in the '581 patent of encrypting only a portion of the request message. *See* Pet. Reply 18–19; Tr. 67:8–68:20. At the hearing, Petitioner argued that one of ordinary skill in the art would have understood that only a portion of the message need be encrypted. Tr. 67:8–68:20. Petitioner, however, fails to provide any persuasive evidence in support of this reading of the claim in view of the express claim language and the description in the Specification.

Petitioner thus provides no basis to allow for a portion of the request message to be unencrypted. *See generally* Pet. 48–50; Pet. Reply. 18–19.

Claim 4 requires that the request message (not just a portion thereof) is encrypted, and Petitioner fails to show that Ishiyama's request message (which includes the unencrypted outer packet's source address) meets this requirement. Ex. 1001, 11:6; *see also In re Hiniker Co.*, 150 F.3d 1362, 1369 (Fed. Cir. 1998) ("[T]he name of the game is the claim.").

Furthermore, during the oral hearing, Petitioner repeated its argument that Ishiyama's request message is encrypted because the encapsulated packet is encrypted, even though the outer packet's header is unencrypted. *See* Tr. 27:9–11, 30:3–11. Having an unencrypted outer packet "would be just like [what] the claims would require, as well, because you can't send a request message without having an outer packet that's unencrypted," according to Petitioner. *Id.* at 30:12–16. Put differently, Petitioner argued:

> [T]he request message that's being sent is encrypted. The outer header isn't encrypted, but the rest of the message is. And there's a reason why the outer header isn't encrypted: because it can't be. If the outer header was encrypted, then the message wouldn't be able to be sent because nobody would be able to know what the destination and source addresses are. So, of course, the outer header isn't encrypted, but the rest of the message is, in fact, encrypted.

Id. at 27:9–16. We are not persuaded by Petitioner's argument that Ishiyama teaches this limitation because the outer header cannot be encrypted. First, Petitioner does not point to any evidence to support this argument, and thus, we do not credit it. *See In re Geisler*, 116 F.3d 1465, 1470 (Fed. Cir. 1997) (explaining that attorney arguments and conclusory statements that are unsupported by factual evidence are entitled to little probative value).

Second, even if we consider this argument, Petitioner conflates a request message that includes its unencrypted outer packet as a part of the request message (such as in Ishiyama) with a request message that does not (e.g., a request message that is contained wholly within the encrypted encapsulated packet), and Petitioner does not account for the latter. *E.g.*, Tr. 27:9–16, 30:12–16. Nor does Petitioner provide any argument or evidence to show that an example request message (i.e., "a registration request (RREQ)") disclosed in the '581 patent is not wholly within the encrypted encapsulated packet. *See generally* Pet.; Pet. Reply; *see also* Ex. 1001, 7:43–62.

Accordingly, Petitioner has not demonstrated by a preponderance of the evidence that claim 4 of the '581 patent would have been obvious to one of ordinary skill in the art in view of Ishiyama and Murakawa.

F. Challenged Claims 6 and 7

Claims 6 and 7 depend from claim 5. Ex. 1001, 11:15–21. Claim 5 recites "[t]he method of claim 1 wherein the method further comprises the security gateway sending back *a reply message* to the mobile terminal at the second address to confirm the address change." Ex. 1001, 11:11–14 (emphasis added). The Petition does not address claim 5's reply message in its showing for claims 6 and 7. *See* Pet. 50–54. Nor does the Petition allege that this asserted ground (Ishiyama and Murakawa) renders claim 5 unpatentable. Instead, the Petition challenges claim 5 based on another ground (Ishiyama, Murakawa, and Ahonen), and relies on Ahonen to teach claim 5's reply message. Pet. 54–61; *see also infra* Section VII(B) (discussing Petitioner's challenge of claim 5 as obvious over Ishiyama, Murakawa, and Ahonen). The Petition does not contend that claims 6 and 7 are obvious over Ishiyama, Murakawa, and Ahonen. *See* Pet. 54–61.

We agree with Patent Owner that "Petitioner's assertion that claims 6–7 are unpatentable under [Ishiyama and Murakawa] . . . fails because it does not account for the limitations of intervening claim 5." PO Resp. 63–64 (citing Pet. 50–54). Moreover, we disagree with Petitioner that Patent Owner makes a "form-over-substance argument" and "improperly tak[es] too stringent of a reading of the Petition." Pet. Reply 22–23.

The Petition guides the proceeding. *See Koninklijke Philips N.V. v. Google LLC*, 948 F.3d 1330, 1335–36 (Fed. Cir. 2020). The Federal Circuit explained that "Congress chose to structure a process in which it's the petitioner . . . who gets to define the contours of the proceeding," and that "the statute envisions that a petitioner will seek an *inter partes* review of a particular kind—one guided by a petition describing 'each claim challenged' and '*the grounds on which the challenge to each claim is based*.'" *Id.* at 1335 (quoting *SAS Inst. Inc. v. Iancu*, 138 S. Ct. 1348, 1355 (2018) (quoting 35 U.S.C. § 312(a)(3))) (emphasis added). "Although the Board is not limited by the exact language of the petition, . . . the Board does not 'enjoy[] a license to depart from the petition and institute a *different* inter partes review of his own design.'" *Id.* at 1336 (quoting *SAS*, 138 S. Ct. at 1356) (citing *Sirona Dental Sys. GmbH v. Institut Straumann AG*, 892 F.3d 1349, 1356 (Fed. Cir. 2018)).

Here, the Petition alleges that claims 6 and 7 are obvious in view of Ishiyama and Murakawa. Pet. 4, 50–54. In other words, the combination of Ishiyama and Murakawa is "the grounds on which the challenge to [these] . . . claim[s] is based.'" *Koninklijke Philips*, 948 F.3d at 1335. In view of how the Petition is worded and the analysis provided for claims 6 and 7, we do not consider one of the challenged grounds to be whether claims 6 and 7 would have been obvious in view of Ishiyama, Murakawa, *and Ahonen*.

We are not persuaded by Petitioner's argument that "*inter partes* reviews are notice based proceedings," and that Patent Owner "had notice of [Petitioner's] arguments since the beginning of this proceeding." Pet. Reply 25 (citing *Sirona Dental*, 892 F.3d at 1356; Pet. 50–54, 61–64). Nor are we persuaded by Petitioner's argument that if Patent Owner "believe[s] there is a deficiency in the art relating to the limitations of claims 6-8 . . ., [Patent Owner] ha[d] sufficient opportunity to address any purported deficiencies in its sur-reply." *Id.* (citing *Sirona Dental*, 892 F.3d at 1356). Again, it is the Petition that guides the proceeding. *See Koninklijke Philips*, 948 F.3d at 1335–36. Furthermore, any statements in the Decision on Institution regarding the sufficiency of Petitioner's showings for claims 6 and 7 were preliminary. *See Trivascular, Inc. v. Samuels*, 812 F.3d 1056, 1068 (Fed. Cir. 2016) ("At th[e Institution] point, the Board is considering the matter preliminarily without the benefit of a full record. The Board is free to change its view of the merits after further development of the record . . . ."). Upon a review of the full record, and in light of *Koninklijke Philips*, we find that Petitioner's showings for claims 6 and 7 are insufficient for the reasons we provide herein.

We also are not persuaded by Petitioner's argument that "Ahonen is not needed to show the unpatentability of the limitations recited in claims 6[and 7] because claims 6[and 7] do not further limit the elements recited in claim 5 and instead only limit elements that appear in claim 1." Pet. Reply 23. Rather, "[c]laims in dependent form shall be construed to include all the limitations of the claim incorporated by reference into the dependent claim."

37 C.F.R. § 1.75(c). In other words, claims 6 and 7 include claim 5's requirements regarding the reply message. *Id.* The Petition fails to account for the claimed reply message in its analysis of claims 6 and 7, and thus, does not demonstrate their unpatentability. Pet. 50–54.

We also are not persuaded that the Petition presents, "as an alternative theory, [that claim 5 is] . . . unpatentable over the combination of Ishiyama and Murakawa due to the well-known 'ACK' functionality used in the TCP/IP protocol taught by Ishiyama." Pet. Reply 22 (citing Pet. 54–55; Ex. 1022 ¶¶ 63–65). Rather, the Petition provides that "in the TCP/IP protocol, destination computers receiving data packets are required to transmit positive acknowledgments (ACK) to source computers to provide a reliable and secure IP connection." Pet. 55. More specifically, Petitioner argues that "[t]he TCP must recover from data that is damaged, lost, duplicated, or delivered out of order by the internet communication system[, and that t]his is achieved by assigning a sequence number to each octet transmitted, and requiring a positive acknowledgment (ACK) from the receiving TCP." *Id.* at n.8 (quoting Ex. 1012, 4; citing Ex. 1002 ¶ 120).

This argument — which appears in a separate ground (Ishiyama, Murakawa, and Ahonen) — fails to show that Ishiyama teaches an ACK that is sent to a mobile terminal's second address to confirm an address change, as required by claim 5. Nor does Petitioner tether this argument to any specific portions of Ishiyama or Murakawa. Pet. 55. To the contrary, Petitioner admits that "Ishiyama and Murakawa . . . do not explicitly describe this reply message." *Id.* Petitioner further admits that "after an address update request message has been sent from a mobile terminal, Ishiyama and Murakawa do not describe how a mobile terminal would be informed that the address was successfully updated before initiating communications from the new address." *Id.* at 55–56 (citing Ex. 1002 ¶ 123). Petitioner's analysis of claim 5 under this ground addresses what Ahonen adds to the combination of Ishiyama and Murakawa. *Id.* at 55–61. Petitioner does not assert that claim 5 is obvious over Ishiyama, Murakawa, and the knowledge of ACK functionality in the TCP/IP protocol. *Id.* at 4 (summarizing ground as obviousness over Ishiyama, Murakawa, and Ahonen), 54–61 (analyzing ground as including Ahonen).

Nevertheless, even if we consider the Petition to include an assertion that claim 5 is unpatentable as obvious over Ishiyama and Murakawa (without adding Ahonen), we are not persuaded that Petitioner made such a showing. Specifically, we are not persuaded by Petitioner's argument that in light of the TCP's ACK that "the reply message as recited in claim[] . . . 5 was obvious as a concept in the prior art and would have been obvious in view of Ishiyama and Murakawa." *Id.* at 55; *see also* Ex. 1002 ¶ 122. Although "[a] person of ordinary skill in the art is also a person of ordinary creativity, not an automaton," *KSR*, 550 U.S. at 421, there may be limits in a particular case as to how much gap-filling may be based on such creativity. *See Arendi S.A.R.L. v. Apple Inc.*, 832 F.3d 1355, 1361–63 (Fed. Cir. 2016); *DSS Tech. Mgmt., Inc. v. Apple Inc.*, 885 F.3d 1367, 1374–75 (Fed. Cir. 2018) (reliance on ordinary creativity to supply a missing limitation requires the same "searching" inquiry as reliance on common sense). We find that Petitioner fails to provide persuasive evidence that one of ordinary skill in the art would have found it obvious to send a reply message to a mobile terminal's second address to confirm an address change in view of TCP's ACK.

We do not credit Dr. Goldschlag's declaration testimony that claim 5's reply message "would be an obvious concept to confirm the successful updating of the address at the security gateway," and that "in view of the well-known TCP/IP protocol, . . . [one of ordinary skill in the art] would have understood that a reply message would be an obvious implementation detail in view of Ishiyama and Murakawa." Ex. 1002 ¶ 122. Dr. Goldschlag's discussion of TCP using ACKs to address data that is damaged, lost, duplicated, or delivered out of order does not provide sufficient factual corroboration for these opinions concerning using ACKs in the context of address updating. Ex. 1002 ¶ 120 (citing Ex. 1012, 4); *see also In re Am. Acad. of Sci. Tech Ctr.*, 367 F.3d 1359, 1368 (Fed. Cir. 2004) ("[T]he Board is entitled to weigh the declarations and conclude that the lack of factual corroboration warrants discounting the opinions expressed in the declarations."); 37 C.F.R § 42.65(a). Dr. Goldschlag also opines that "a mobile terminal that moves to a new address would expect to receive an acknowledgment or confirmation message before transmitting packets from its new address," and that "[a] mobile terminal would likely not blindly transmit data packets from its new address without first receiving confirmation that the security gateway is ready to accept data packets from the new address." Ex. 1002 ¶ 120. We likewise do not credit this testimony, as it too lacks sufficient factual corroboration, and is contrary to the '581 patent's teaching that a reply message is "optional." *See* Ex. 1001, 9:66–10:1, 10:6.

We also disagree with Petitioner that Patent Owner's Response "explicitly recognized" Petitioner's "alternative theory" that claim 5 was obvious "due to the well-known 'ACK' functionality used in the TCP/IP protocol taught by Ishiyama." Pet. Reply 22. Rather, the alternative theory Patent Owner responds to is based on Ishiyama's "message (7) from the correspondent host to the mobile terminal in Ishiyama's Figure 7." PO Resp. 72 (citing Pet. 59–61; Ex. 1004, Fig. 7). For this theory, Petitioner argues that in operation 7 "the destination of the message is 'CoA2' and confirms the updated address of the mobile computer." Pet. 60 (citing Ex. 1004, 12:66–13:5). Petitioner argues that "[u]sing CoA2, the correspondent host 3 may originate communications sent to the mobile computer 2 at the updated Care-of address." *Id.* (citing Ex. 1004, 13:6–9). We are not persuaded by Petitioner's arguments. Rather, we agree with Patent Owner and find that "the message in step (7) is simply an encapsulated message using the new care-of address CoA2 in the outer packet[, and] . . . is not a [confirmatory] reply to a request for an address change from the mobile terminal." PO Resp. 72; *see also* Ex. 1004, Fig. 7, 12:66–13:5. Moreover, Ishiyama does not teach that operation 7's message is recognized as a confirmation of the address change. Ex. 1004, Fig. 7, 12:66–13:9. Instead, Ishiyama simply sends and receives messages at the second address (e.g., correspondent host sends a secure message to the mobile computer). *Id.* at Fig. 7, 12:66–13:5; *see also id.* at 13:3–5 ("Consequently the session is guaranteed even when the mobile computer 2 moves (the operations (6) and (7) of FIG. 7)."); *infra* Section VI(G) (discussing Ishiyama teaching claim 9's security gateway forwarding the message as an encrypted secure message to the second address).

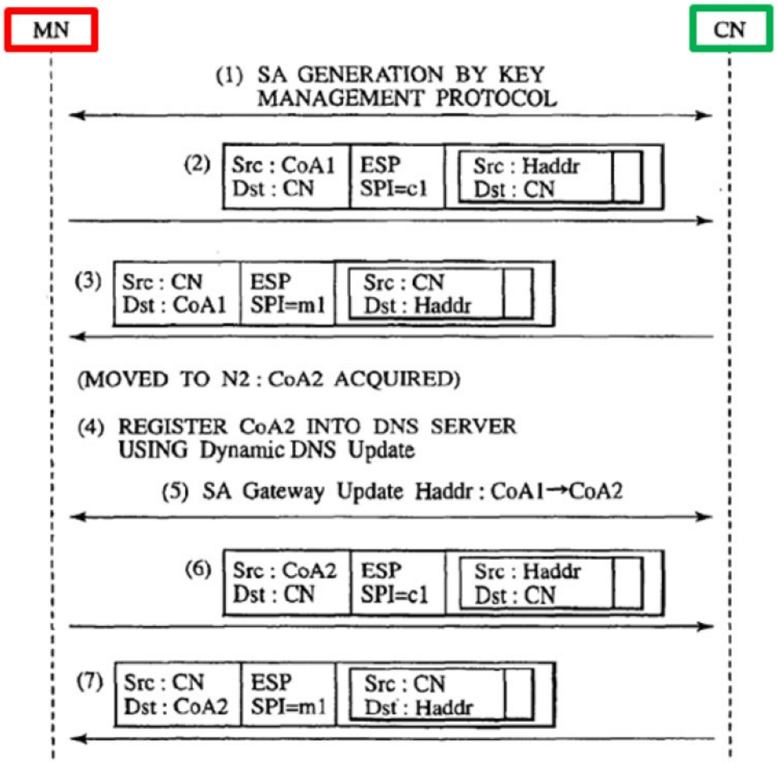
Accordingly, Petitioner has not demonstrated by a preponderance of the evidence that claims 6 and 7 of the '581 patent would have been obvious to one of ordinary skill in the art in view of Ishiyama and Murakawa.

G. Challenged Claim 9

Claim 9 is an independent claim and shares some nearly identical limitations with independent claim 1. Namely, claim 9's preamble and first four elements are nearly identical to those recited in claim 1. *Compare* Ex. 1001, 12:1–17, *with id.* at 10:50–67. As such, the parties rely on their arguments from claim 1 for these limitations. Pet. 41–42; PO Resp. 65. As these limitations are the same, and the parties rely on their same arguments, our findings as to claim 1's preamble and first four limitations apply equally here. *See supra* Section VI(C)(1)–(5). Accordingly, we find that Petitioner has demonstrated by a preponderance of the evidence that the combination of Ishiyama and Murakawa teaches claim 9's preamble and first four limitations.

In addition, claim 9 further recites "the other terminal sending a message to the second address of the mobile terminal via the security gateway, and the security gateway receiving the message from the other terminal and forwarding the message as an encrypted secure message to the second address." Ex. 1001, 12:18–22. We agree with Petitioner and find that the combination of Ishiyama and Murakawa teaches these limitations. Pet. 41–47.

We find that Ishiyama teaches sending a secure message from Ishiyama's correspondent host to the mobile computer's second location, as shown below in Figure 7's operation (7), as annotated by Petitioner. *See* Pet. 41–42 (annotating Ex. 1004, Fig. 7).

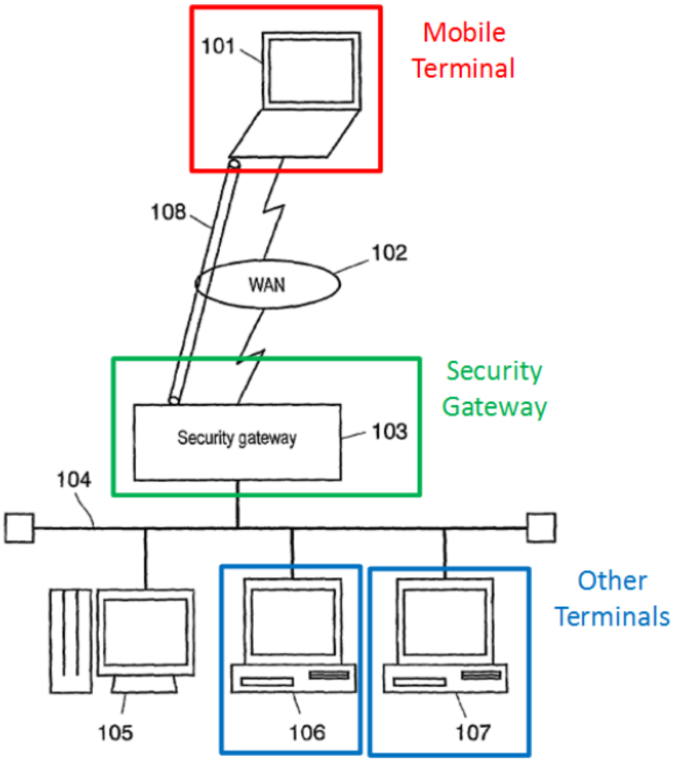

MN
CN
(1) SA GENERATION BY KEY MANAGEMENT PROTOCOL
(2) Src : CoA1 Dst : CN | ESP SPI=c1 | Src : Haddr Dst : CN
(3) Src : CN Dst : CoA1 | ESP SPI=m1 | Src : CN Dst : Haddr
(MOVED TO N2 : CoA2 ACQUIRED)
(4) REGISTER CoA2 INTO DNS SERVER USING Dynamic DNS Update
(5) SA Gateway Update Haddr : CoA1→CoA2
(6) Src : CoA2 Dst : CN | ESP SPI=c1 | Src : Haddr Dst : CN
(7) Src : CN Dst : CoA2 | ESP SPI=m1 | Src : CN Dst : Haddr

Annotated Figure 7 "is a sequence chart showing an exemplary processing sequence in the case where the mobile computer initiates communications at a visited site and then changes . . . location" with a green box around the correspondent node ("CN") identifier and a red box around the mobile computer identifier ("MN"). Ex. 1004, 5:20–23; Pet. 42 (annotating Ex. 1004, Fig. 7). Ishiyama teaches that as a result of its CoA update operations, "at the correspondent [host] currently communicating with the mobile computer 2, the endpoint of the IPSEC tunnel is changed from 'CoA1' to 'CoA2' as the destination of all the security associations,'" and "[c]onsequently, the session is guaranteed even when the mobile computer 2 moves . . . ." Ex. 1004, 12:66–13:5; Pet. 41–42. Put differently, as Figure 7 illustrates, the secure message is sent to the second address of the mobile terminal from Ishiyama's correspondent host. Ex. 1004, Fig. 7

(illustrating for operation (7) that the outer packet's Src: has the value "CN" and Dst: has the value "CoA2").

As to Murakawa, we agree with Petitioner and find that Murakawa teaches an "other terminal" sending a secure message in a secure connection to an address of a terminal via the security gateway, and that the security gateway receives the message from the "other terminal" and forwards it as an encrypted secure message to the terminal's address. *E.g.*, Ex. 1005, Fig. 5; Pet. 44–46. This is shown in Murakawa's Figure 5, shown below as annotated in the Petition. *See* Pet. 44 (providing annotated Figure 5).

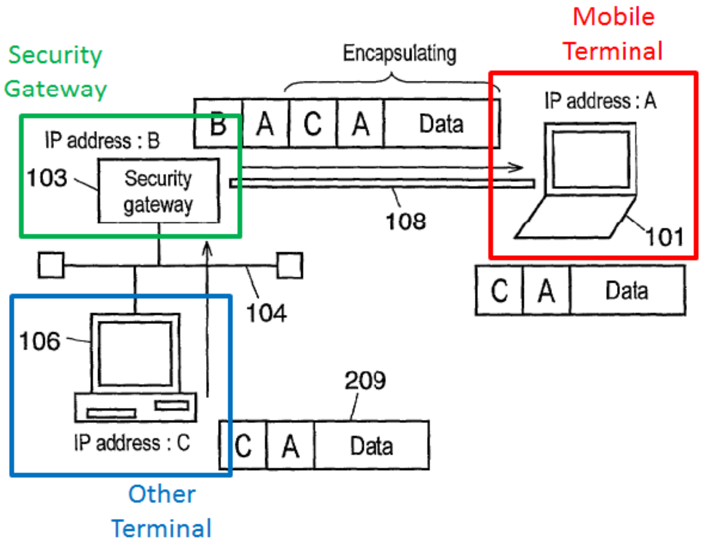
FIG. 5 PRIOR ART



Murakawa's Figure 5, as annotated by Petitioner, shows a "prior art typical network system" with (i) a red box around PC 101 and labeled "Mobile Terminal," (ii) a green box around security gateway 103 and labeled "Security Gateway," and (iii) a blue box around each of PC 106 and

PC 107, and labeled "Other Terminals." Ex. 1005, 4:32–33; Pet. 44 (annotating Ex. 1005, Fig. 5). As illustrated in Figure 5, Murakawa teaches that an "other terminal" (PC 106) sends a secure message in the secure connection (VPN 108) to the mobile terminal (PC 101) via security gateway 103. *Id.* at 1:61–2:4, 2:62–65, Fig. 5; *see also supra* Section VI(C)(1) (discussing our findings regarding Figure 5's teachings). Furthermore, Figure 8, shown below as annotated in the Petition, also illustrates the addressing of the secure message sent from PC 106 (other terminal) to the PC 101 (mobile terminal) by security gateway 103.

FIG. 8 PRIOR ART



Annotated Figure 8 "illustrates diagrammatically . . . prior art IPsec communication in the tunnel mode" with (i) a red box around PC 101 and labeled "Mobile Terminal," (ii) a green box around security gateway 103 and labeled "Security Gateway," and (iii) a blue box around PC 106, and labeled "Other Terminal." Ex. 1005, 4:41–42; Pet. 45 (annotating Ex. 1005, Fig. 8). As illustrated, "IP addresses 'A', 'B', and 'C' are assigned to PC

101, security gateway 103, and client PC 106, respectively." Ex. 1005, Fig. 8, 3:4–6; Pet. 45. Murakawa teaches the following:

> When client PC 106 on LAN 104 transmits an IP packet to PC 101, which has established connection with PC 106 via VPN 108,
>
> 1) client PC 106 generates IP packet 100 in which the sender's IP address is "C" and the receiver's IP address is "A", then sends it to security gateway 103;
>
> 2) received packet 100, gateway 103 identifies that the packet is the one to be sent to PC 101 which has established VPN 108;
>
> 3) gateway 103 encapsulates IP packet 100 according to exchanged information during the IKE communication;
>
> 4) the IP header including the sender's IP address B and the receiver's IP address "A" is added to outside the originally set IP address;
>
> 5) authentication information is added to the encapsulated IP packet based on the exchanged information, then the IP packet is encrypted;
>
> 6) received the encapsulated packet via VPN 108, PC 101 retrieves encapsulated original IP packet 100 from the received packet, according to the exchanged information, then process[es] it.

Ex. 1005, 3:8–28; Pet. 45–46. In other words, Murakawa teaches an "other terminal" (PC 106) sending a secure message in a secure connection to an address of a mobile terminal via the security gateway. Ex. 1005, 3:8–28. Furthermore, we credit Dr. Goldschlag's testimony that one of ordinary skill in the art would have understood that Murakawa teaches a well-known IPSec tunnel mode configuration with a security gateway facilitating communication between a mobile terminal and other terminals because this testimony is consistent with our findings of Murakawa's teachings. *See* Ex. 1002 ¶ 99.

Accordingly, we find that the combination of Ishiyama and Murakawa teaches the "other terminal" (PC 106) sending a secure message in the secure connection (VPN 108) to the second address (CoA2) of the mobile terminal via security gateway 103, and that the security gateway 103 receives the message from other terminal (PC 106) and forwards the message as an encrypted secure message (via VPN 108) to the second address of the mobile terminal.

We are not persuaded by Patent Owner's arguments that Ishiyama's "operation (7) is an end-to-end, two-component secure communication from correspondent terminal CN to mobile terminal MN," and does not teach "[t]he three-component communication called for by the claim (other terminal-security gateway-first terminal)." PO Resp. 66–67 (citing Ex. 2009 ¶¶ 157–159). Patent Owner focuses on Ishiyama's teachings individually, rather than the combined teachings of Ishiyama and Murakawa. *See In re Merck & Co.*, 800 F.2d 1091, 1097 (Fed. Cir. 1986) ("Non-obviousness cannot be established by attacking references individually where the rejection is based upon the teachings of a combination of references"). Again, as to the second way Petitioner combines Ishiyama and Murakawa, Ishiyama's mobile address changing functionality is combined with Murakawa's security gateway configuration (e.g., security gateway 103 and other terminal 106). *See* Pet. 11–53; Dec. on Inst. 25, 38–39 (noting the two alternative ways). Hence, a mobile terminal securely communicates with another terminal via Murakawa's security gateway 103 rather than Ishiyama's correspondent host 3. *See* Pet. 11–53.

In summary, we find combining Ishiyama's mobile address changing functionality with Murakawa's security gateway and another terminal teaches "the other terminal sending a message to the second address of the mobile terminal via the security gateway, and the security gateway receiving the message from the other terminal and forwarding the message as an encrypted secure message to the second address."

Lastly, we find that the parties' arguments and our findings concerning a rationale to combine Ishiyama and Murakawa discussed above in the context of claim 1 apply equally here. *See supra* Section VI(C)(7) (finding that one of ordinary skill in the art would have combined the references). Accordingly, we find by a preponderance of the evidence that Petitioner has provided persuasive reasoning showing that one of ordinary skill in the art would have had reason to combine Ishiyama and Murakawa in the manner claimed.

Accordingly, based on a review of the entire record, we find that Petitioner has demonstrated by a preponderance of the evidence that claim 9 would have been obvious over the combined teachings of Ishiyama and Murakawa.

VII. ALLEGED OBVIOUSNESS OVER ISHIYAMA, MURAKAWA, AND AHONEN

Petitioner argues that the combination of Ishiyama, Murakawa, and Ahonen renders claims 3 and 5 of the '581 patent obvious under 35 U.S.C. § 103(a). Pet. 54–61. We have reviewed the parties' arguments and the evidence of record. For the reasons that follow, we determine that Petitioner shows by a preponderance of the evidence that claims 3 and 5 would have been obvious to one of ordinary skill in the art in view of Ishiyama, Murakawa, and Ahonen.

A. Summary of Ahonen

Ahonen relates to a VPN "in which a mobile terminal establishes a secure connection with a correspondent host located in an intranet, via a [s]ecurity [g]ateway." Ex. 1006, 1:5–7. Figure 1, shown below, illustrates this network topology, in accordance with Ahonen's invention. *Id.* at 3:30–31, 3:57–61.

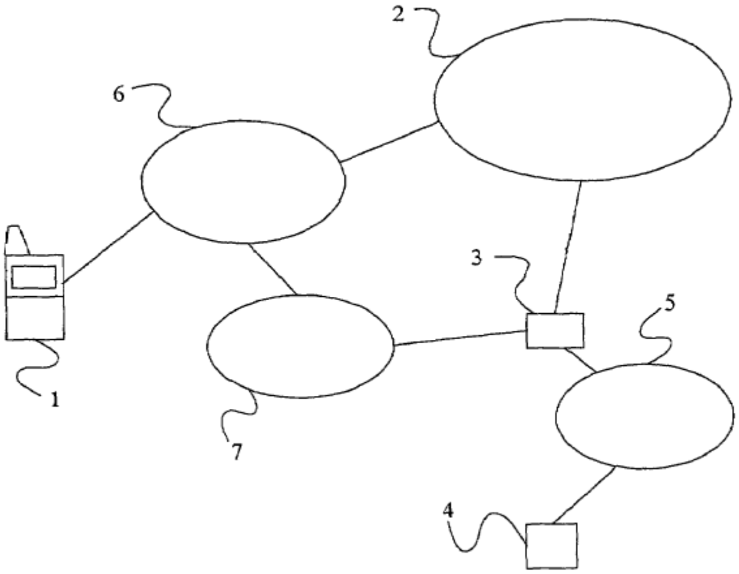


Figure 1

Figure 1 illustrates mobile host 1 connected to correspondent host 4 via access network 6, Internet 2, firewall 3, and intranet 5. *Id.* at 3:57–63. A secure connection is established between mobile host 1 and correspondent host 4 over this path. *Id.* at 3:65–4:1.

B. Challenged Claims 3 and 5

Claims 3 and 5 depend from independent claim 1. Claim 3 recites "[t]he method of claim 1, wherein in step c) a reply back to the mobile terminal is sent from the security gateway after the request from the mobile terminal to change the address." Ex. 1001, 11:6–8. Claim 5 recites "[t]he method of claim 1 wherein the method further comprises the security gateway sending back a reply message to the mobile terminal at the second address to confirm the address change." *Id.* at 11:11–14. We agree with Petitioner and find that the combination of Ishiyama, Murakawa, and Ahonen teaches the subject matter of claims 3 and 5. Pet. 54–61.

First, for the reasons we explain above, we agree that the combination of Ishiyama and Murakawa teaches the subject matter of claim 1, from which claims 3 and 5 depend.

Second, we agree with Petitioner and find that Ahonen teaches that a mobile host moves to another address and sends a certificate to a security gateway (also referred to as a firewall) using an IPsec protocol. Ex. 1006, 3:58–59, 9:29–30, 9:40; Pet. 57. Ahonen teaches that the certificate sent from the mobile host may contain "the cryptographic identity of the mobile host" and "the (New) Source and Destination IP addresses (if changed)." Ex. 1006, 9:33–35; Pet. 57. The firewall then determines whether a corresponding database includes a record matching the identification of the mobile host. Ex. 1006, 9:52–61. Ahonen teaches that if a match is found, the database is updated (e.g., "the Source and Destination IP addresses are updated if they are changed"), and the firewall "send[s] an 'ACK' (acknowledgement) message back to the mobile host." *Id.* at 9:62–65, 10:4–6; Pet. 57. Ahonen teaches that after the mobile host has received the "ACK" message from the firewall, the mobile host can begin to send application traffic. Ex. 1006, 10:21–25.

Third, we agree with Petitioner and find that one of ordinary skill in the art would have found it obvious to implement Ahonen's reply ACK message with Ishiyama's address changing functionality to aid in maintaining "mobility without interrupting the session" as in Ishiyama. Pet. 58 (citing Ex. 1006, 6:54–60). We also agree with Petitioner that one of ordinary skill in the art would have found it obvious to incorporate Ahonen's teachings to "inform the mobile computer whether the records stored at the security gateway were successfully updated to allow the mobile computer to begin transmitting data packets," as taught in Ahonen. *Id.*, Ex. 1006, 10:4–7, 10:21–25. *See PGS Geophysical*, 891 F.3d at 1365 ("[T]he motivation to modify a reference can come from the knowledge of those skilled in the art, from the prior art reference itself, or from the nature of the problem to be solved.").

We are not persuaded by Patent Owner's argument that "Ahonen cannot satisfy the 'reply' limitation" because Ahonen's underlying request is "for a **new secure connection with a new SA** that can accommodate an address change," rather than "for an **existing secure connection with the same SA** to be modified to accommodate the change in the IP address of the mobile terminal." PO Resp. 71 (citing Ex. 2009 ¶¶ 181–183). Nor are we persuaded by Patent Owner's argument that Ahonen's reply message follows a request for changing a secure connection between a mobile terminal and a correspondent host, rather than a secure connection between a mobile terminal and a gateway. PO Resp. 71–72 (citing Ex. 1006, 8:33–36; Ex. 2009 ¶ 183). For both of these arguments, Patent Owner incorrectly focuses on Ahonen's teachings individually, rather than the combined teachings of Ishiyama, Murakawa, and Ahonen. *See Merck*, 800 F.2d at 1097 ("Non-obviousness cannot be established by attacking references individually where the rejection is based upon the teachings of a combination of references"). Again, Petitioner combines Ishiyama's mobile address changing functionality with Murakawa's security gateway configuration (e.g., security gateway 103 and other terminal 106). *See* Pet. 12–54; Dec. on Inst. 24–25, 37–38 (noting the two alternative ways). And, Ahonen's reply message is incorporated into this combination where (i) Ishiyama's address changing functionality combined with Murakawa's security gateway configuration relates to an existing secure connection with the same SA, and (ii) Murakawa's security gateway sends the reply message to the mobile terminal. Pet. 17–47, 54–58.

Accordingly, Petitioner has demonstrated by a preponderance of the evidence that claims 3 and 5 of the '581 patent would have been obvious to one of ordinary skill in the art in view of Ishiyama, Murakawa, and Ahonen.

VIII. ALLEGED OBVIOUSNESS OVER ISHIYAMA, MURAKAWA, AND FORSLÖW

Petitioner argues that the combination of Ishiyama, Murakawa, and Forslöw renders claim 8 of the '581 patent obvious under 35 U.S.C. § 103(a). Pet. 61–64. Claim 8 is a dependent claim and depends from claim 5. Ex. 1001, 11:22–23. As we discuss above, claim 5 recites, *inter alia*, "a reply message," which the Petition does not address in its showing for claim 8. *See supra* Pet. 61–64. Again, the Petition alleges that claim 5 is obvious in light of Ishiyama, Murakawa, and Ahonen, and relies on Ahonen to teach claim 5's reply message. Pet. 54–61; *see also supra* Section VII(B) (discussing Petitioner's challenge of claim 5 as obvious over Ishiyama, Murakawa, and Ahonen). But this asserted ground for claim 8 does not include Ahonen.

As explained above, the Petition guides the proceeding. *See Koninklijke Philips*, 948 F.3d at 1335–36. Here, the Petition alleges that claim 8 is obvious in view of Ishiyama, Murakawa, and Forslöw. Pet. 4, 61–64. In other words, the combination of Ishiyama, Murakawa, and Forslöw is "the ground[] on which the challenge to [the] . . . claim is based.'" *Koninklijke Philips*, 948 F.3d at 1335. In view of how the Petition is worded and the analysis provided for claim 8, we do not consider one of the challenged grounds to be whether claim 8 would have been obvious in view of Ishiyama, Murakawa, Forslöw, *and Ahonen*.

Accordingly, as the Petition does not address claim 5's requirements regarding the "reply message" for this asserted ground, we find that Petitioner has not demonstrated by a preponderance of the evidence that claim 8 of the '581 patent would have been obvious to one of ordinary skill in the art in view of Ishiyama, Murakawa, and Forslöw.

IX. CONCLUSION[17]

Based on the full record before us, we determine that Petitioner has demonstrated by a preponderance of the evidence that (i) claims 1, 2, and 9 of the '581 patent are unpatentable under 35 U.S.C. § 103(a) in view of Ishiyama and Murakawa; and (ii) claims 3 and 5 are unpatentable under 35 U.S.C. § 103(a) in view of Ishiyama, Murakawa, and Ahonen. We also determine that Petitioner has not demonstrated by a preponderance of the

[17] Should Patent Owner wish to pursue amendment of the challenged claims in a reissue or reexamination proceeding subsequent to the issuance of this decision, we draw Patent Owner's attention to the April 2019 *Notice Regarding Options for Amendments by Patent Owner Through Reissue or Reexamination During a Pending AIA Trial Proceeding*. *See* 84 Fed. Reg. 16,654 (Apr. 22, 2019). If Patent Owner chooses to file a reissue application or a request for reexamination of the challenged patent, we remind Patent Owner of its continuing obligation to notify the Board of any such related matters in updated mandatory notices. *See* 37 C.F.R. § 42.8(a)(3), (b)(2).

evidence that (i) claims 4, 6, and 7 of the ’581 patent are unpatentable under 35 U.S.C. § 103(a) in view of Ishiyama and Murakawa; or (ii) claim 8 is unpatentable under 35 U.S.C. § 103(a) in view of Ishiyama, Murakawa, and Forslöw.

Claim(s)	**35 U.S.C §**	**Reference(s)/Basis**	**Claims Shown Unpatentable**	**Claims Not Shown Unpatentable**
1, 2, 4, 6, 7, 9	103(a)	Ishiyama, Murakawa	1, 2, 9	4, 6, 7
3, 5	103(a)	Ishiyama, Murakawa, Ahonen	3, 5	
8	103(a)	Ishiyama, Murakawa, Forslöw		8
Overall Outcome			1–3, 5, 9	4, 6–8

X. ORDER

In consideration of the foregoing, it is hereby

ORDERED that, pursuant to 35 U.S.C. § 314(a), Petitioner has shown by a preponderance of the evidence that claims 1–3, 5, and 9 of the ’581 patent are unpatentable;

FURTHER ORDERED that Petitioner has not shown by a preponderance of the evidence that claims 4 and 6–8 of the ’581 patent are unpatentable; and

FURTHER ORDERED that parties to the proceeding seeking judicial review of this Final Written Decision must comply with the notice and service requirements of 37 C.F.R. § 90.2.

PETITIONER:

Michael D. Specht
Daniel S. Block
Timothy L. Tang
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.
mspecht-ptab@sternekessler.com
dblock-ptab@sternekessler.com
ttang-ptab@sternekessler.com

PATENT OWNER:

James T. Carmichael
Stephen Schreiner
CARMICHAEL IP LAW, PLLC
jim@carmichaelip.com
schreiner@carmichaelip.com

Christopher J. Lee
Richard B. Megley
Brian E. Haan
Ashley E. LaValley
LEE SHEIKH MEGLEY & HAAN LLC
clee@leesheikh.com
rmegley@leesheikh.com
bhaan@leesheikh.com
alavalley@leesheikh.com

Kenneth J. Weatherwax
Patrick Maloney
Jason C. Linger
LOWENSTEIN & WEATHERWAX LLP
weatherwax@lowensteinweatherwax.com
maloney@lowensteinweatherwax.com
linger@lowensteinweatherwax.com